**CECOM Drawing A 3285412**

# Joint Tactical Radio System (JTRS)

# Wideband Networking Waveform (WNW)

# Functional Description Document (FDD)

## Version 2.21
## 29 November 2001

JTRS Joint Program Office
1700 N. Moore ST., Suite 1000
Arlington VA 22209

# Table of Contents

**Section** **Page**

# List of Figures

# List of Tables

# Section 1
# JTRS Wideband Networking Waveform Employment

## 1.1 Overview

The purpose of this document is to define a Wideband Networking Waveform (WNW) requirement for the Joint Tactical Radio System (JTRS). JTRS is a program to define and acquire a family of software programmable radios. The JTRS products will be designed in accordance with the Software Communications Architecture (SCA). The JTRS architecture enables many legacy and newly developed radio waveforms to use common system components (hardware and software) and coexist in one box.

The WNW for JTRS represents a new capability for the Department of Defense as described in the JTRS Operational Requirements Document (ORD). The WNW addresses many of the networking requirements in the JTRS ORD. The WNW must include or support:

- Interoperability between the Services,
- Seamless delivery of video, voice, and data services,
- Adaptation to user message requirements or network conditions,
- Ad hoc formation of scalable networks,
- Automatically (waveform controlled) and manually (user controlled) adaptable RF or routing features,
- Standard protocols and interfaces if possible,
- Evolutionary implementation of requirements and simple insertion of new capabilities.

The WNW design process should fully utilize the Application Programming Interfaces (APIs), modularity, and SCA features of the JTRS during its development. The design should include standardized APIs at each layer of the waveform to provide an easy mechanism for iterative performance improvements and overall waveform evolution with advancing technology developments.

Minimum required values are provided where required. Where values are not given, vendors may propose trade-offs in order to provide the best overall performance.

## 1.2 Army JTRS WNW Network Employment

The Army objective for the JTRS WNW is to provide the lower tactical Internet (TI) backbone. The lower TI architecture is a 2-tier architecture as illustrated in figure 1.2.1. The two tiers refer to subnets as the first tier (i.e. SINCGARS nets) and the backbone refers to the second tier connecting all the subnets together. The initial application of the WNW would be to provide the backbone function of the lower TI. Eventually, the WNW could replace the first tier also.

In addition, the JTRS WNW may be used to support the Warfighters Information Network – Tactical (WIN-T) Tactical Operation Center (TOC) to TOC communication requirements.

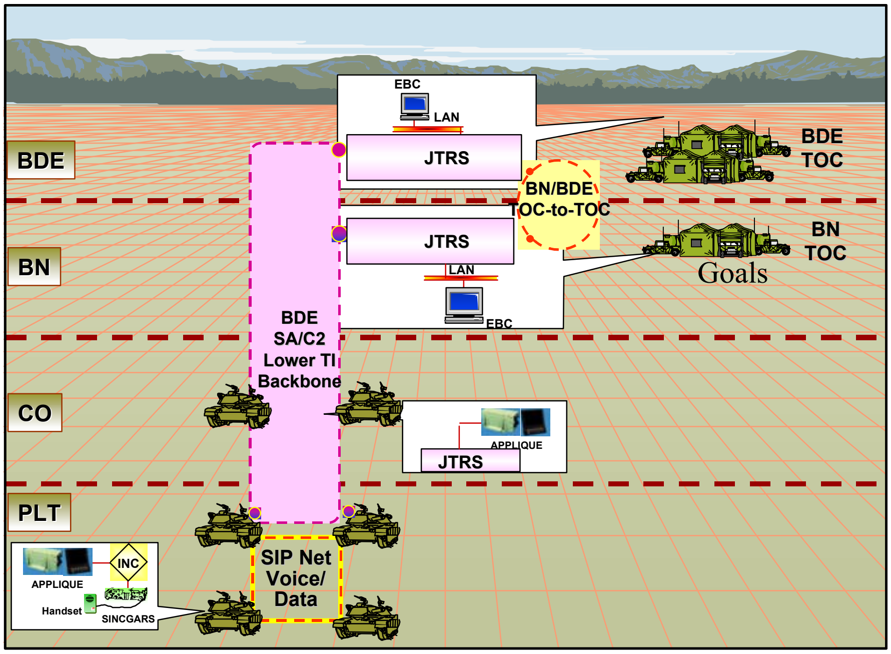

**Figure 1.2.1 Army use of the JTRS Wideband Waveform(s)**

### 1.2.1 Network Size

The WNW network will provide data communications service to mobile and quasi-stationary subscribers within the Division. It will serve Upper Echelon TOCs and Lower Echelon Force units with one or more networks. The number of radios on the network(s) needed to satisfy this service, as shown below, assumes one radio is a node on the network(s) at which several hosts can use its services. The radio or node as used here implies that part of the JTRS radio that performs the JTRS wideband networking service.

#### 1.2.1.1 Upper Echelon TOC Requirements

The number of radios needed to serve the Upper Echelon TOCs for the WIN-T TOC-TOC requirement on a Division wide network is approximately 130. This number consists of approximately 20 radios that operate in Division TOCs and approximately 25 radios at TOCs within each Brigade.

#### 1.2.1.2 Lower Echelon Force Requirements

The number of radios needed to satisfy the Lower Echelon Force elements for a Division wide network is approximately 1500. This number consists of approximately 200 radios that operate within a Brigade size force. With attachments, a Brigade size force can grow to approximately 350 radios. A requirement of the network that services the Lower Echelon is to be a backbone that interconnects numerous stub networks such as SINCGARS networks. Most Lower Echelon force units (Platoon, Company, etc) have two JTRS wideband data radios that serve the unit.

#### 1.2.1.3 Division wide JTRS Wideband Network

The quantity of data radios for a network that satisfies both Upper and lower Echelon requirements would be approximately the sum of each, or 1630.

### 1.2.2 Operational Area Coverage

A Division deploys over a diverse terrain area of 200 kilometers (km) wide and 150 km deep. The area of coverage for the Upper Echelon TOC to TOC network is approximately the upper third of the Division area or 10,000 square kilometers (km$^2$). The area of coverage for the Lower Echelon network is approximately the lower two thirds of the Division area or 20,000 km$^2$. When a Brigade size force is deployed for division operations within a division operational area, the Brigade area of coverage is approximately 6,500 sq. km. When a Brigade is deployed as a separate entity, the area of coverage for a Brigade is approximately 100 km x 100 km.

## 1.3 Navy JTRS WNW Network Employment

The Navy's current networked communications strategy is the Joint Maritime Communications Strategy (JMCOMS). Within JMCOMS, the Automated Digital Network System (ADNS) connects the Integrated Shipboard Network System (ISNS) onboard ships with other remotely located DoD networks using the ship's RF communications systems. ADNS is designed to enable end user systems employing commercial standard interfaces and protocols (i.e. Internet Protocols), to exchange data as if on the same physical network. A candidate Amphibious Readiness Group (ARG) ADNS deployment architecture including JTRS WNW capability is shown in Figure 1.3.1.

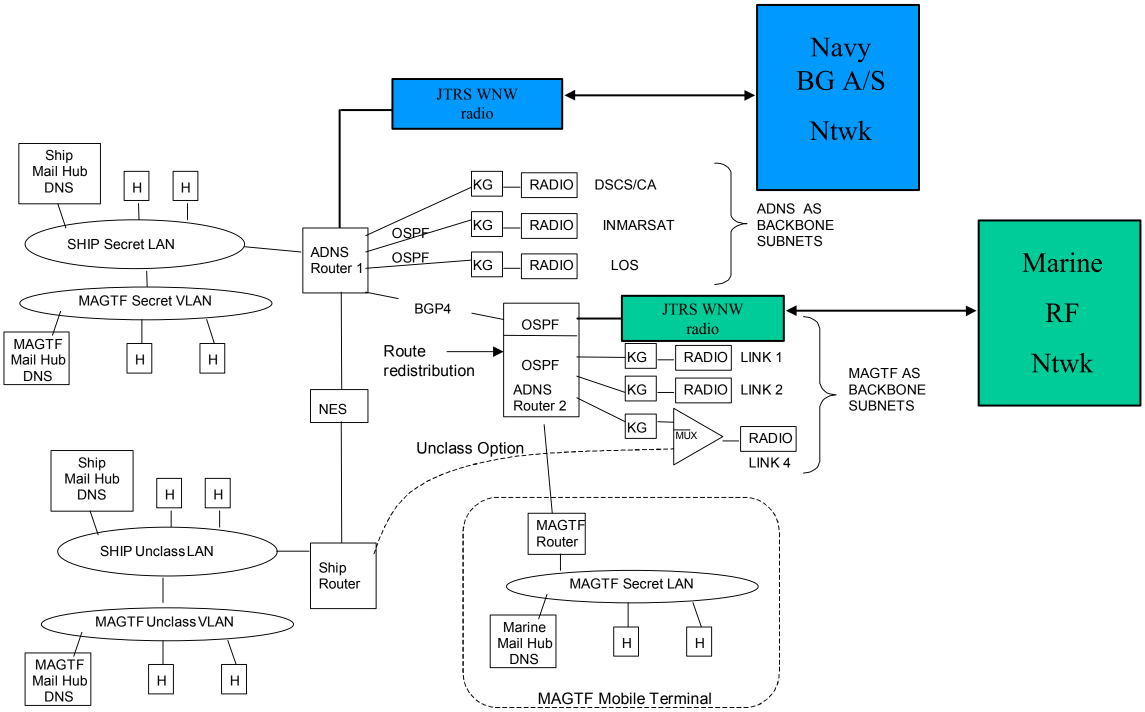

**Figure 1.3.1 ARG ADNS Architecture with JTRS WNW**

### 1.3.1 Network Size

A Navy Battle Group (BG) or ARG includes air, surface, and subsurface platforms. The BG/ARG has the capability to dominate air, surface, and subsurface threats.

#### 1.3.1.1 Navy Battle Group Requirements

A typical BG consists of 7 – 15 maritime platforms which may include various combinations of the following hull types: a carrier (CV/CVN), command ship (LCC, AGF, MCS), surface combatants (CG, DDG, DD, FFG), submarines (SSN), logistics ships (AOE), and a carrier air wing consisting of 75-80 aircraft. A typical air wing has three FA-18 squadrons, one F-14 squadron, one S-3 squadron, one EA-6B squadron, one E-2C squadron, and one helicopter squadron. The E-2C is the airframe targeted for JTRS as well as any unmanned aerial vehicle (UAV) deployed with the

BG. There are three E-2Cs in an air wing. Other naval air platforms that may have JTRS include the H-60s helicopters. Each Navy hull and certain aircraft in the BG will need at least one JTRS WNW channel to support Tier 2 tactical mobile network backbone communications. Additional WNW channels may be allocated and used as either backup channels, or as extra WNW channels to increase bandwidth. The BG will require 15 – 30 JTRS WNW nodes.

#### 1.3.1.2 Navy Amphibious Readiness Group Requirements

A typical ARG consists of 3 – 6 maritime platforms and can be bulked up to 24 platforms for a Marine Expeditionary Force (MEF) sized landing force. Platforms include a Multi-purpose Amphibious Assault Ship (LHA/LHD), a Landing Platform Dock (LPD), a Landing Ship Dock (LSD), several surface combatants for force protection and naval fires (CG, DDG, DD), and a Marine Expeditionary Unit (MEU) consisting of 2,000 Marines, or 15,000 – 25,000 Marines for an MEF, and their embarking equipment (helicopters, AV-8B Harriers, vertical take-off UAVs (VTUAVs), AAAVs, tanks, HMMWVs,etc.). Each Navy hull and certain Navy and Marine aircraft, and VTUAVs in the ARG/MEU will need at least one JTRS WNW channel to support Tier 2 tactical mobile network backbone communications. Additional WNW channels may be allocated and used as either backup channels, or as extra WNW channels to increase bandwidth. The Navy's participation in the ARG will require 6 – 12 JTRS WNW nodes.

### 1.3.2 Operational Area Coverage

A Naval BG/ARG "owns" an operational coverage area that is 300 nmi in radius from the BG/ARG. This includes open ocean operational areas, as well as littoral operational areas and the air space above each. The JTRS WNW will need to support a widely distributed sparse network topology with pockets of clustered nodes throughout the Area of Coverage. Airborne JTRS WNW nodes will be used to relay/route data between beyond line of sight (BLOS) WNW nodes. Operational Maneuver from the Sea (OMFTS) describes this Naval Forces scenario. The three-tiered communications architecture for OMFTS is depicted in Figure 1.3.2. JTRS WNW represents Tier 2 in this USN communication architecture to support backbone subnet links.

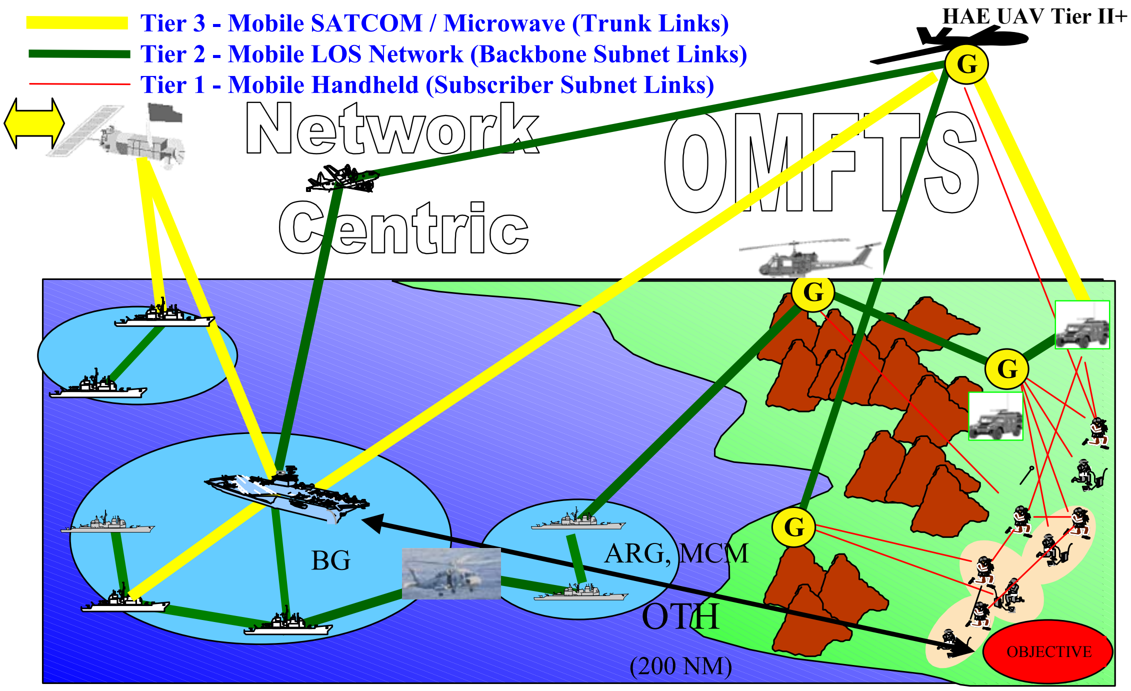
Tier 3 - Mobile SATCOM / Microwave (Trunk Links)
Tier 2 - Mobile LOS Network (Backbone Subnet Links)
Tier 1 - Mobile Handheld (Subscriber Subnet Links)
HAE UAV Tier II+
Network Centric
OMFTS
G
G
G
G
BG
ARG, MCM
OTH
(200 NM)
OBJECTIVE

**Figure 1.3.2 Naval Forces OMFTS Scenario**

## 1.4 Marine Corps JTRS WNW Network Employment

The Marine Corps views JTRS as the key component to its tactical communications infrastructure within the operational area. Depending on the radio's size, weight, and power requirements the WNW will be employed in a variety of ways. The primary role will be connecting Combat Operations Centers (COCs), whatever the size, from mobile units such as ground (HMMWV, LAV, AAAV) and airborne (MV-22, helicopter) to more static large tent encampments and shipboard. The JTRS WNW must provide interlaced voice, data, and video. JTRS radios implementing the WNW will be placed into UAVs (e.g. VTUAV) and other relay platforms in order to provide over the horizon connectivity. When the WNW can be instantiated in a radio the size and weight of a manpack form-factor, it will be employed down to platoon and reconnaissance-sized units. When the WNW can be implemented on a radio the size and weight of a hand-held form-factor, it will be used down to the squad level. At these lower echelons the radio will need to provide interconnection within units and provide automatic relays to other units.

Fig. 1.4.1 is a top-level view of the OMFTS C4ISR systems architecture. In short, it consists of a large number of low-power wireless local area networks (WLANs) interconnected by a self-organizing wide area network (WAN) of JTRS. To prevent fragmentation of the network due to distance or terrain, airborne relay nodes augment the terrestrial portion of the WAN backbone. Finally, a multi-source Marine Air-Ground Task Force (MAGTF) broadcast service is used for wide-area broadcast and multicast traffic. Note that each WLAN has a primary and at least one alternate wireless access point/gateway. Clearly, this scheme requires automatic promotion of alternate access points when the primaries fail or move beyond line of sight.

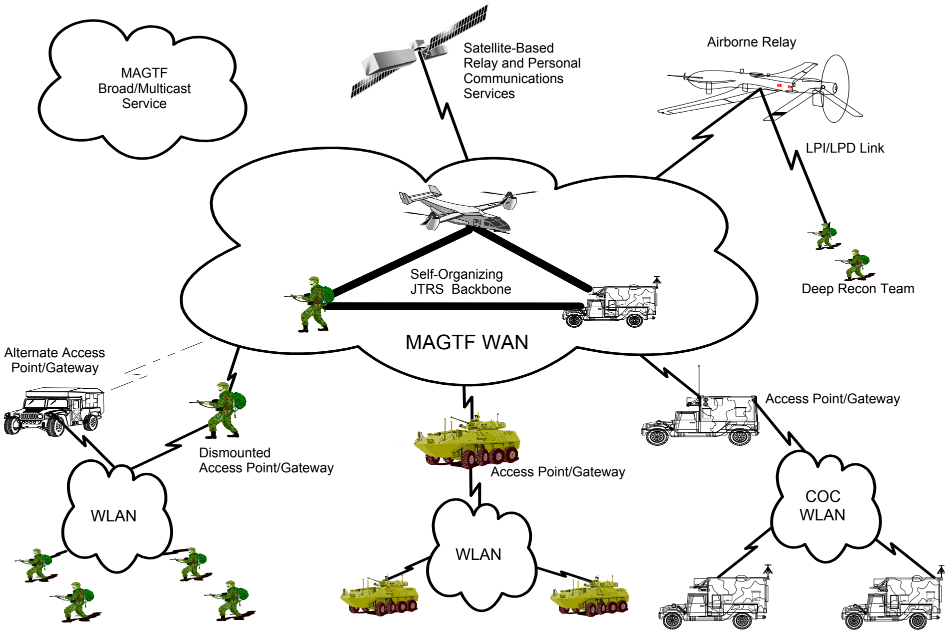
MAGTF Broad/Multicast Service
Satellite-Based Relay and Personal Communications Services
Airborne Relay
LPI/LPD Link
Self-Organizing JTRS Backbone
Deep Recon Team
MAGTF WAN
Alternate Access Point/Gateway
Dismounted Access Point/Gateway
Access Point/Gateway
Access Point/Gateway
WLAN
WLAN
COC WLAN

**Figure 1.4.1 OMFTS Communication Envisioned Architecture**

Each battalion-sized and larger unit (units with a staff) may deploy with a Combat Operations

Center (COC) consisting of two or more COC modules. These COC modules serve as mobile operational facilities containing a router, at least one file server, multiple generic workstations connected to a vehicle LAN, integral power and air conditioning, and at least one JTRS radio. Wireless bridges will be used to interconnect all COC modules in a given unit COC, thus allowing passengers in separate vehicles to function as a single staff. An important aspect of this architecture is that all classes and classifications of traffic share the same network backbone. In other words, voice, video, and data share the same switching and transmission systems, regardless of their level of classification (e.g. secret or unclassified).

Ship To Objective Maneuver (STOM) will require that dispersed forces are able to coordinate air, fire support, maneuver, and logistics activities between themselves and central controlling agencies for each functional area. Control agencies may be co-located or assigned to subordinate commanders for operational control. Under conventional warfare, the next senior commander coordinated each functional area resulting in a hierarchical flow of information. Thus, hierarchical communications links were traditionally established. While traditional command centers may be established ashore during sustained operations, the communications architecture must allow for the dynamic establishment of networks (both voice and data) between multiple organizations. The architecture must be able to adapt to environmental and organizational changes in forming communications paths.

## 1.4.1 Network Size

The JTRS WNW has two objectives: COC and lower echelon objectives.

### 1.4.1.1 Combat Operations Center (COC)

For regimental-sized operations in a mid-intensity conflict, it is envisioned that 25 – 30 mobile command posts will be operating in a region.

### 1.4.1.2 Lower Echelon Forces

The inclusion of lower echelon forces increases the number of network nodes to between 150 and 340 nodes. The JTRS WNW deployment will initially be used solely to provide the backbone connectivity but may in the future be used to support individual platforms.

## 1.4.2 Operational Area Coverage

An amphibious task force must be able to operate and control forces up to 250 km ashore and communicate with naval forces up to 150 km at sea. The force must control an area wide enough to provide protection to the landing force enroute to the objective and to provide sustainment once the objective is seized. This could extend to 100 km wide. Airborne relays may be used to support the range. But under OMFTS, the goal is to minimize dependence on communications relays.

## 1.5 Air Force JTRS WNW Network Employment

The Air Force will use the JTRS WNW to provide a seamless extension of the Global Grid Network to Air Force users requiring wireless network connectivity. The WNW will provide high throughput, dynamically adaptable connectivity for exchange of IP-based voice, data, and video traffic. The WNW should support efficient and reliable interconnection between terrestrial (fixed and mobile) and airborne users of the Global Grid Network in a changing network topology without introducing gateway bottlenecks. The WNW will support network nodes on mobile and airborne platforms (as well as deployed and fixed platforms) without the need of the intervention of the personnel on those platforms.

The WNW will be robust and adaptable to support communications connectivity during rapidly changing distances and orientations between nodes and operation in the following environments: (1) co-site environments typical of C2, ISR, and other communications intensive airborne and ground platforms, (2) tactical RF propagation environments, and (3) use RF spectrum suitable for worldwide operation.

The WNW routing capability will be robust and flexible to support dynamically changing network topologies and radio silent subscribers. The routing capability in both ground and airborne nodes must interface to commercial routing and network planning processes and systems used by the Air Force (including those used with wideband satellite communications networks) that are provided external to JTRS.

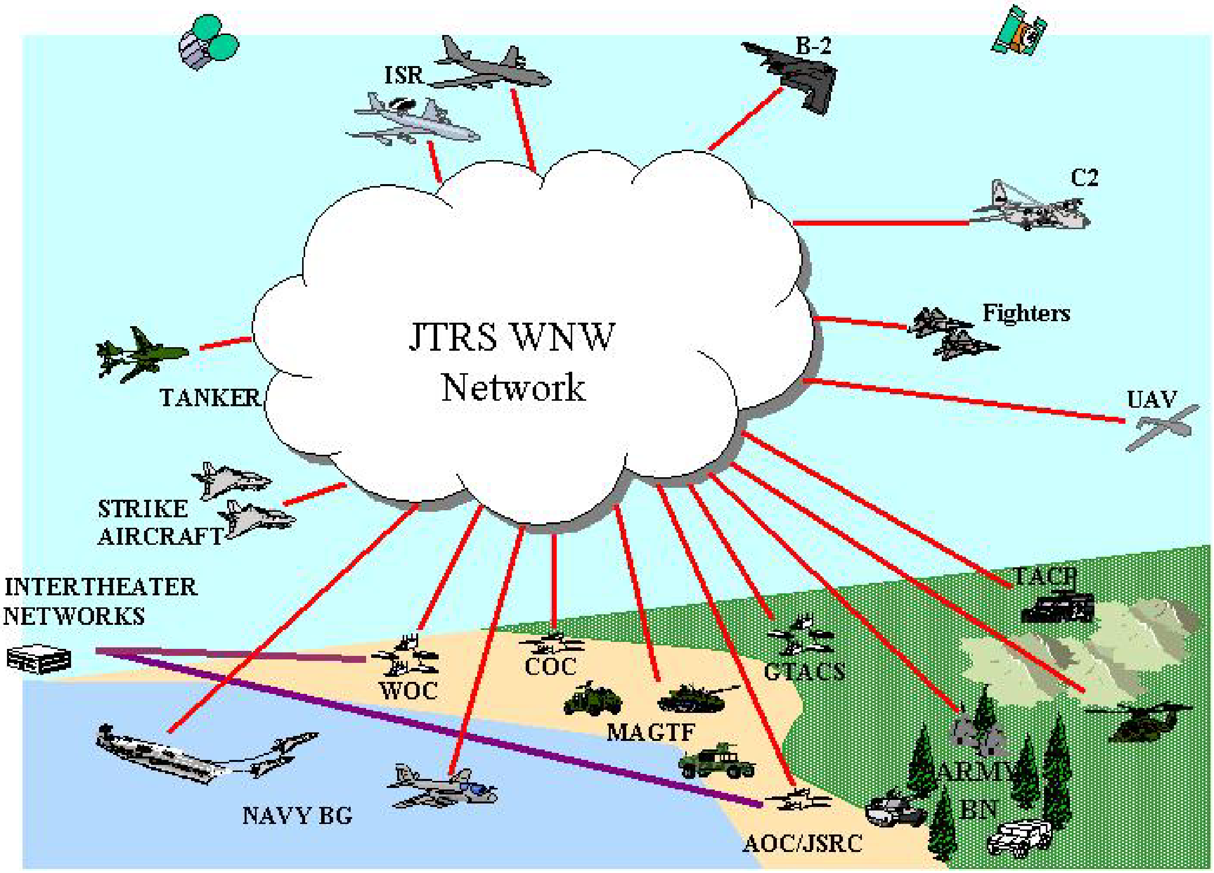

**Figure 1.5.1 Air Force use of the Wideband Networking Waveform**

### 1.5.1 Network Size

The JTRS WNW will provide network services to ground (fixed, deployed, and mobile) and airborne nodes operating in a theater-size geographical area. The network will include intra-Air Force as well as Joint participants. The total number of Air Force JTRS radios on the network could range between 100 and 250 based on deployment of an Aerospace Expeditionary Force (AEF) of 75 aircraft, ground support and command and control operational facilities, on-call Aerospace Expeditionary Wing (AEW) of 100 aircraft, high demand low density aircraft, and fixed and/or deployed operational facilities. Up to 75 airborne nodes could participate in a network at any given time. The remainder of the nodes will be ground-based. Some nodes may participate in more than one JTRS WNW network simultaneously.

### 1.5.2 Operational Area Coverage

The JTRS WNW will provide network services to ground (fixed, deployed, and mobile) and airborne nodes in a theater-size geographical area of approximately 1000 nmi by 1000 nmi. Node-to-node ranges that must be supported within this area of operation are provided in paragraph 2.3.1. Theater and worldwide network connectivity will be supported by internetworking with IP-based networks on wireless and terrestrial media.

# Section 2

# Operating Requirements

## 2.1 WNW Operation

The JTRS WNW network shall provide connectivity in an operational area through self-forming, self-healing mobile ad hoc networking. The JTRS WNW network shall support worldwide connectivity by inter-networking with IP-based networks on other media. The JTRS WNW shall support both backbone links (tier 2) and subnet links (tier 1) as described in Section 1 and defined in Appendix D Part II – Terms and Definitions.

Further waveform requirements that are generic to all JTRS waveforms can be found in CECOM Drawing A3285420

## 2.2 Special Operating Modes

The JTRS WNW shall have parameters and functions that support special operating modes specified in paragraphs 2.2.1 through 2.2.5. These modes are required for various operational conditions.

### 2.2.1 Gateway Networking Mode

The JTRS WNW shall automatically perform a gateway function between the backbone links (Tier 2) and the subnet links (Tier 1). The gateway function shall include communications between the WNW network and nodes operating in the Asymmetric Networking Mode and the LPI/LPD Networking Mode.

### 2.2.2 Asymmetric Networking Mode

The JTRS WNW shall automatically perform asymmetric transmission rates between JTRS WNW nodes. Data packet transmission between different nodes shall be optimized on a packet by packet basis to support various RF channel conditions.

### 2.2.3 Receive-only Networking Mode

The JTRS WNW shall support a receive-only (radio silent) operation function at one or more nodes that require emission control (EMCON). The receive-only function shall be initiated when operationally required by the network control manager or the JTRS operator. A JTRS WNW node operating in this mode shall not transmit any RF information on the network. The JTRS WNW shall facilitate smooth transition to and from the receive-only and normal operations. The JTRS WNW shall continue to forward data to any host or any router attached to the JTR Set. JTR Sets not operating in the receive-only mode must be able to recognize which JTR Sets are using receive-only mode so that messages can be routed to them in the absence of routing updates. To accomplish this, nodes transitioning to receive-only networking mode may send "going silent" announcements to other nodes on the network. Such transmissions, however, are permitted only when they are compatible with the security requirements of the node transitioning to this mode of operation. The receive-only node must be able to rejoin the network as specified in paragraph 3.1.2. Provisions may be made to prevent packet transmissions to nodes that left the network, but are not operating in the radio silence mode.

### 2.2.4 LPI/LPD Networking Mode

A JTRS WNW node operating under covert conditions shall be capable of joining and participating in the WNW network using a low probability of intercept/low probability of detection (LPI/LPD) function. The LPI/LPD function shall be initiated when operationally required by the network control manager or the JTRS operator. In this mode of operation, the node shall perform the network control handshaking/signaling that is necessary to join the network. This LPI/LPD node shall have minimal impact on the data rate of the WNW network nodes on the backbone of the WNW network that are not operating in LPI/LPD mode.

### 2.2.5 Point-to-Point Mode

The JTRS WNW shall support a point-to-point operation mode that optimizes the throughput and latency between two nodes.

## 2.3 Information Rates

The performance of the waveform shall be sufficient to support the operational scenarios described in section 1 using the Message Performance Requirements in Appendix B. Test scenarios based upon the employments within Section 1 will be provided by the JTRS JPO. Appendix C provides additional test scenarios that shall be used to verify performance.

### 2.3.1 Data Rates

The JTRS WNW shall be capable of automatically adaptable data rates. The JTRS WNW shall provide negotiated automatic fallback to lower data rates for degraded channel conditions or restricted modes of operation. Conversely, the JTRS WNW shall provide negotiated automatic step-up in data rates for improved channel conditions, to and from each node.

### 2.3.2 User Throughput Rates

The JTRS WNW should provide sufficient throughput to support user requirements for a broad range of data, voice, and video applications in a mobile network. The JTRS WNW shall support user throughputs greater than 2 Mbps as a Threshold and 5 Mbps as an Objective in Test Scenario 1a, 1b, 1c and 1d described in Appendix C. The JTRS WNW shall support user throughputs greater than 1 Mbps as a Threshold and 2 Mbps as an Objective in Test Scenario 2a, 2b, 2c and 2d described in Appendix C.

### 2.3.3 Network Throughput Rates

Using Test Scenarios 3 through 5 specified in Appendix C and the message performance requirements in Appendix B the WNW shall support greater than 2 Mbits per second of Network Throughput as a threshold. The WNW shall have the ability to make efficient use of extra frequency spectrum when available and shall support Network Throughputs of greater than 5 Mbits per second as an objective.

### 2.3.4 Point-to-Point Mode Throughput Rate

The JTRS WNW operating in the Point-to-Point mode shall support a user throughput rate of greater than 1 Mbps as a Threshold and 2 Mbps as an Objective in each direction.

## 2.4 Performance Characteristics

### 2.4.1 Range

When using antennas and power levels suitable for the respective host platforms, the JTRS WNW line-of-sight point-to-point range shall meet the following requirements:

| | |
|---|---|
| Air-to-Air* | at least 370 km (200 nmi) |
| Air-to-Ground/Surface* | at least 370 km (200nmi) |
| Ground-to-Ground | at least 10 km (5.4 nmi) |
| Ship-to-Ship | at least 28 km (15 nmi) |
| Ship-to-Shore | at least 28 km (15 nmi) |

*These ranges apply to aircraft flying at altitudes where RF propagation will be unaffected by terrain, foliage, or other features. For aircraft flying at altitudes where terrain, foliage, or other features may affect RF propagation, the WNW network must provide ranges between such low flying aircraft or between these aircraft and ground WNW network nodes at least that of the ground-to-ground requirement above. However, the WNW must still support communication between these low flying aircraft and command and control aircraft, such as the Airborne Warning and Control System, up to the air-to-air range given above.

### 2.4.3 Packet Error Rate

The JTRS WNW shall provide a packet error rate of less than 0.1% in a back-to-back laboratory configuration with receive signal levels between –100 dBm to –10 dBm. Tests shall be measured with packet sizes of 64 bytes, 576 bytes and 1500 bytes in Test scenarios 1a, 1b, 1c, 1d, 2a, 2b, 2c, and 2d described in Appendix C.

### 2.4.4 Power Control

The JTRS WNW shall automatically control power to reduce the amount of interference and allow for frequency reuse.

### 2.4.5 Terrain/Propagation Environment

The JTRS WNW shall be able to operate in all tactical RF propagation environments such as hilly, mountainous, dense vegetation, desert, and urban terrain. The JTRS WNW shall be robust and adaptable to support connectivity during rapidly changing distances and orientations between nodes. The JTRS WNW shall adapt to the presence of Doppler effects, fading, multipath, and other RF channel conditions in the operating environments and host platform operating profiles.

### 2.4.6 Spectrum Allocation

The JTRS WNW shall use RF spectrum that satisfies technical, operational, and regulatory requirements for worldwide operation. The WNW operating frequency range shall include frequency sub-bands allocated to the mobile radio communications service that are authorized for military use. Since the frequency bands satisfying these criteria may vary by region, the WNW and host JTR Sets shall incorporate adequate flexibility with respect to operating frequency, bandwidth, modulation, and power to address a range of possible host nation restrictions. See Appendix A for additional guidance.

The Wideband Networking Waveform shall have the capability for automatic transmit frequency lockouts. The lockout frequencies shall be programmable to specific center frequencies that would prohibit any transmissions within plus or minus 25 kHz from the specified center frequency.

The lockout frequencies shall have the capability to be grouped into categories, such as:
1) Safety of Life
2) Go to War - wartime frequency releasable list (WFRL)
3) Command Defined

### 2.4.7 Noise Environment

The JTRS WNW shall be able to operate in tactical RF propagation environments. These propagation environments include unintentional (atmospheric, background, self-interference, and co-site interference) and intentional (jamming) noise. The JTRS WNW shall be able to operate in co-site environments typical of C2, ISR, and other communications-intensive platforms (both airborne and surface) as well as within line-of-sight of other wireless/radio networks, radar, and navigation systems. The JTRS WNW network should be able to operate while sharing an antenna with other radio channels.

### 2.4.8 Anti-Jamming Capabilities

The JTRS WNW shall include an anti-jam (AJ) feature of operation for protection to prevent the enemy disruption of services.

# Section 3
# Networking Requirements

The JTRS WNW will be used in widely varying scenarios. These will range from a few radios in a small area, few radios in a fairly large area, many radios in a small area to many hundreds of radios spread over a large area. In any network there could be a mixture of very short distances and very long distances between radios. The environments will range from desert to urban to mountainous to at sea. Some deployments may have single links joining areas of nodes to form a large network. The goal for the link layer and networking protocols is to support a system that is flexible enough such that the same basic waveform and networking protocols can be used for all scenarios. Optimization for each scenario should be achieved through configuration parameters requiring little or no management intervention.

## 3.1 WNW Network Performance

The WNW shall provide self-organizing, self-healing networks capable of responding to dynamic changes in connectivity. The WNW network shall provide routing and management protocols/schemes that can rapidly respond to ad hoc changes in network topology caused by such things as node addition and deletion, node movements, antenna shadowing or orientation, terrain masking, or interference. The performance of the waveform shall be sufficient to support the operational scenarios described in section 1 using the Information Exchange Requirements in Appendix B. Test scenarios based upon the employments within Section 1 will be provided by the JTRS JPO. Appendix C provides additional test scenarios that shall be used to verify performance.

### 3.1.1 Network Timing

The WNW network shall still be able to operate if GPS timing is not available.

### 3.1.2 Network Formation

#### 3.1.2.1 Network Size

The WNW network shall have the capability to integrate an initial network of 150 nodes spread over the operational area into a single network within 15 minutes of system initialization.

#### 3.1.2.2 Network Join Time

The WNW network shall have the capability to automatically add one node to an existing network in less than one minute of the node's request to join the network. and up to eight nodes simultaneously within two minutes.

#### 3.1.2.3 Topology

The WNW network shall integrate any node operating in the area of operation into the network. The nodes may be operating at altitudes of between sea level and 65,000 feet above sea level.

#### 3.1.2.4 Network Reorganization

The WNW network shall support routing and management protocols/schemes that can rapidly respond, without excessive overhead, to ad hoc changes in network topology caused by such things as node addition and deletion, node movements relative to other surface or airborne nodes, antenna shadowing, terrain masking, or interference. For these ad hoc changes, the WNW network shall provide efficient use of resources while providing adequate performance and without undue organizational or hierarchical restrictions.

The WNW network shall also support network reorganizations introduced through the network management interface within the times shown in Table 3.1.1. For nodes in Receive-only mode, these routing and management protocols/schemes shall not permit routing through these nodes, nor will they respond to route discovery or other network control queries.

**Table 3.1.1 Reorganization Requirements**

| | |
|---|---|
| Move 1 to 4 nodes | 1 min |
| Move 5 to 20 nodes | 5 min |
| Move 21 to 100 nodes | 10 min |

#### 3.1.2.5 Network Self-Healing

The WNW network shall provide traffic rerouting with minimal loss of packets after a change in network topology (e.g., loss of a node or link).

### 3.1.3 Mobility Management

The JTRS WNW network design shall support connectivity to and between ground or surface mobile platforms moving at speeds relative to other platforms in excess of 120 mph while maintaining network connectivity and traffic transmission integrity. The JTRS WNW network design shall support network connectivity and traffic transmission integrity to and between airborne platforms for speeds relative to other platforms up to 900 knots at altitudes of tens of feet to over 65,000 feet above sea level. [Note that the Air Force and other Service airborne platforms will exceed this relative speed at times.] The JTRS WNW network design shall also support connectivity to and between airborne and ground nodes at relative speeds up to 900 knots. The JTRS WNW should maintain stated performance for ship/aircraft pitch, roll, and yaw. The WNW shall maintain stated performance when up to 50% of nodes, limited to a maximum of 75 in any network, are moving at the maximum speeds identified above and a further 50% of all nodes are traveling at speeds up to 80 kilometers per hour.

### 3.1.4 Network Services

The WNW network shall support protocol suites capable of providing the network service requirements below. The WNW network will be used to support unicast, multicast, and broadcast of traffic types to include large data files (>1 Megabyte), video, video teleconferencing, voice, and short or formatted message traffic. These network services shall operate simultaneously.

#### 3.1.4.1 Quality of Service

The WNW shall support Quality of Service (QoS) mechanisms to support differential handling of traffic classes according to their service requirements. The mechanisms shall include precedence handling that discriminates among traffic based on its mission importance. To support an integrated mix of traffic types, including a variety of data, voice, and video, in a variety of operating conditions, the ability to preset and negotiate QoS parameters should be supported. At a minimum, the WNW shall support both DiffServ(RFC 2474) and IP Precedence (RFC 791).

#### 3.1.4.2 Data Precedence

The WNW shall provide preferential treatment of user traffic, with respect to both delivery priority and drop priority. Military communications traffic will vary in requirements for delay and reliability of delivery; the WNW network shall provide mechanisms appropriate to support these various delivery requirements. Listed in Appendix B are the five levels of traffic precedence used in the Defense Switched Network. At a minimum, the JTRS WNW shall provide support for an analogous service.

#### 3.1.4.3 Multimedia Traffic

In addition to data traffic, the WNW will carry real-time traffic, including voice and video. Voice and video have strict requirements on delivery delay (latency), delay variation (jitter), and packet drop rates. The WNW shall support QoS mechanisms to ensure optimum performance for multimedia traffic, including data, voice, and video.

#### 3.1.4.4 Multimedia Packet Performance Requirements

In addition to the message latencies and completion rates contained in Table B-1 of Appendix B for data, the WNW network shall satisfy the packet delay and completion rate requirements for multimedia packets in Table B-2 of Appendix B. These requirements apply to individual packets.

## 3.2 WNW Network Functionality

### 3.2.1 Link Layer Performance Requirements

The link layer should employ protocols that make maximum use of the broadcast nature of radio communications. Required characteristics of the WNW link layer shall include 3.2.1.1 through 3.2.1.5.

#### 3.2.1.1 Message Support

The WNW link layer shall support broadcast, multicast, and unicast messages.

#### 3.2.1.2 Channel Access

The WNW link layer shall provide channel access schemes which:

a) Manage access from multiple nodes that are in line of sight of each other;

b) Minimize packet collisions between these nodes or at nodes in line of sight of two transmitting nodes which are not in line of sight ("hidden node" problem);

c) Maximize simultaneous transmission to receivers that are not in line of sight of each other ("exposed node" problem);

d) Provide fair access between nodes transmitting data with the same precedence in the network.

#### 3.2.1.3 Link Layer Addressing

The WNW shall provide standard link layer addressing and messaging schemes that support unicast, multicast, and broadcast transmissions between nodes in line of sight. Transmissions to nodes beyond line of sight may be handled using the appropriate (unicast, multicast, broadcast) routing schemes.

#### 3.2.1.4 Packet Delivery

The WNW link layer shall provide packet delivery schemes that support assured (acknowledged) and best effort (unacknowledged) message delivery. Assured delivery to broadcast or multicast recipients should use network efficient methods. Receive-only nodes will receive only best effort delivery.

### 3.2.2 RF Network Layer Performance Requirements

The WNW network layer should use protocols/schemes designed for highly dynamic wireless networks. Required characteristics of the WNW network layer shall include 3.2.2.1 through 3.2.2.3.

#### 3.2.2.1 Network Layer Addressing

The WNW network shall use Internet Protocol addressing schemes, including support for subnet addressing and unique and group addresses

#### 3.2.2.2 Routing

The WNW network shall use routing protocols/schemes that support:

a) Unicast, multicast, and broadcast transmissions to nodes or users on any part of the WNW network, or on other military or commercial networks;

b) Scalable networks of from 2 to 1,630 nodes which may be densely or sparsely distributed across an operational area;

c) Ad hoc changes in network topologies caused by such things as node addition and deletion, node movements, antenna shadowing, terrain masking, or interference without overwhelming the network with routing overhead information;

d) Nodes with varying functionality/modes

e) Route transit as well as local traffic.

#### 3.2.2.3 Link Management

The WNW shall employ link management schemes that quickly adapt, without excessive overhead, to rapidly varying connectivity status caused by the mobility of each node relative to other ground or airborne nodes.

## 3.3 Military and Commercial Network Interoperability

### 3.3.1 Internetworking

The JTRS WNW network shall support internetworking between WNW networks and IP-based networks on other media (including terrestrial media, wideband SATCOM, and host platform LANs) to support communication with command authorities, out-of-theater sources of information and support, other in-theater networks, or en-route platforms. The interfaces to networks external to the WNW network can occur at surface and airborne nodes.

### 3.3.2 Interface with external baseband Internet Protocol Devices

The WNW shall interface with external networks running standard Internet Protocols, including but not limited to IEEE 802.3, Open Shortest Path First (OSPF), Border Gateway Protocol (BGP) V4, Multicast extension to OSPF (MOSPF), Protocol Independent Multicast (PIM) (sparse mode and dense mode), or Internet Group Management Protocol (IGMP). Any WNW network node interfacing to other military or commercial IP-based networks shall be configurable as an OSPF Area Border Router or Autonomous System Boundary Router. Hardware interfaces required to support these requirements will be specified in the appropriate Service hardware requirements or specification document.

### 3.3.3 Dynamic Internetworking.

When the WNW network fragments (healing through WNW links not possible) and the fragments can be healed through external links (tier 3), the WNW shall support communication between hosts attached to different fragments for both IP unicast and IP multicast data through existing links with the external network. If an external tier 3 network fragments (healing through tier 3 links not possible) and the fragments can be healed through the WNW then the WNW shall support communication between hosts attached to the fragments of the tier 3 network for both IP unicast and multicast data through existing links with the external network.

# Section 4
# Network Management Requirements

## 4.1 WNW Network Management

The WNW network shall dynamically manage itself, permitting members to join and leave the network without manual intervention, and autonomously execute network security features in section 5. The WNW network shall also permit a Network Manager to plan, monitor, and manage the JTRS WNW network or to manually intervene for disaster recovery such as to excise unauthorized or compromised JTRS WNW network members and to have operational control for Over the Air Rekeying (OTAR) of COMSEC, TRANSEC, and other security variables. The WNW Network Manager shall distribute node configuration data from the Network Manager to the appropriate radios.

The WNW shall include functionality sufficient to organize, manage, and dynamically control network connectivity structures, routing mechanisms, bandwidth allocations, and spectrum restrictions. The WNW shall also provide information to and be interoperable with joint network management tools, to allow network managers to remotely identify and configure user access and profile parameters to prioritize users, network access and message delivery.

The JTRS WNW Network Manager shall be DII COE level 6 compliant. The JTRS WNW and associated network manager shall also comply with the Joint Technical Architecture for network management protocols, and should provide interfaces to COTS standards that meet objective functionality, such as Simple Network Management Protocol Version 3 and Common Open Policy Server Protocol.

WNW Network management software shall be modular in design to aid maintainability, reuse, and tailoring use of the network management application package as required by particular users (e.g. Not all users of the network management application will require the planning portion of the network manager on their hardware platform, therefore the planner portion of the network management application may not be provided to those users).

JTRS WNW Network management should require minimal communications bandwidth so that network performance is not significantly impacted. Network management should use a maximum of 1% of available bandwidth.

The JTRS WNW Network Manager shall exchange management information including, but not limited to, the information exchange requirements listed in Appendix F.

## 4.2 JTRS WNW Network Management Interface

The JTRS WNW network shall provide a Network Management (NM) interface to DOD network management tools and processes to plan the WNW network configuration parameters, monitor the network and permit a Network Manager to make real time parameter changes (e.g. to ensure operations only on authorized frequencies, etc.) from anywhere in the battlefield to optimize network performance.

This interface shall consist of a Graphic User Interface (GUI) that provides interoperability to current and proposed network management environments used within the Joint networking arena (e.g., JNMS or service specific network management tools). The Human Computer Interface (HCI) of the JTRS WNW NM interface shall be in compliance with the Department of Defense (DOD) Technical Architecture Framework for Information Management (Vol. 8, DOD HCI Style Guide). The WNW NM GUI shall allow access to network member's operational parameters or database as needed; but unauthorized access shall be denied.

The WNW NM GUI shall provide network configuration information such as location of network devices and maintaining information on how devices or objects are configured. It shall display a physical representation of the network. The NMT shall be capable of overlaying all network nodes on a map background of the Area of Responsibility using approved symbology in accordance with the JTF Symbol Set. The map background shall use the Military Grid Reference System and Latitude/Longitude, but not simultaneously. This display capability shall allow the network manager to use a map background for planning purposes such as profiling radio links, and allow the network manager the capability to disable the map background once the network is engineered to obtain a logical view of the network. The WNW NM shall provide the capability to view selective groups of nodes or zoom into an area of the network. The WNW NM shall also provide the capability to collect and save the JTRS WNW network traffic statistics. Threshold and performance information shall include parameters for intra-network as well as external interfaces.

The WNW NM shall use service defined Common Hardware Software (CHS). The system design should minimize human performance errors, interface problems and workload (physical, cognitive, attention) requirements. It should be as uncomplicated and intuitive as possible and should include concerted attention to such characteristics as screen content and layout, menus, help availability, feedback, safeguards and the ready accessibility and procedural steps associated with critical tasks/functions.

## 4.3 WNW Network Planning

The WNW NM shall provide capabilities to assist the network planning process. The NM shall have a system level menu that allows the planner to logically progress through the planning process. Minimum capabilities are listed:

- Provide a tool to automate the process of planning and generating configuration files and defining all the necessary parameters of radios participating in the network.

- Provide a means to distribute or synchronize databases between two or more NMs that monitor and participate in managing the same network. This capability allows the NM to disseminate planning information to all associated network management sites.
- Provide an on-line, real-time chat capability to support fault isolation, troubleshooting, resolution, and connectivity with operators at multiple NM sites.
- Provide the capability to perform automated communications propagation analysis. The NM shall automatically perform the analysis of the propagation loss on the transmission systems and provide feedback, visual and/or hardcopy, to the planner.
- Planner shall be capable of importing text and graphics files created by other office automation applications as necessary to produce network plans and configuration files.

## 4.4 WNW Network Configuration

A capability is needed to transfer the configuration data from the WNW NM to the appropriate radios. The WNW NM shall be able to reconfigure radios during the mission to reflect changing mission requirements.

## 4.5 WNW Network Monitoring

The Network Manager shall monitor and manage the JTRS wideband network using the WNW NM GUI. The WNW NM shall display the nodes of the network and their configuration and operating performance data. This capability, however, should not constrain a WNW network's ability to rapidly respond to ad hoc changes in network topology caused by such things as node addition and deletion, node movements, antenna shadowing or orientation, terrain masking, or interference.

### 4.5.1 Fault Management

The WNW NM shall identify and process events and reported faults. The WNW NM shall provide a fault management capability to detect and alert the user to problem areas, identify and diagnose problems in performance and configuration, provide recommended solutions, and manage and track faults until they are successfully corrected.

### 4.5.2 Performance Management

The WNW NM shall monitor the status of the radios by acquiring and displaying radio performance data. It shall monitor network condition, report changes in status, and respond to evolving network changes. The NM should be able to graphically display the status of the network. The NM shall receive input from devices to obtain utilization and status, monitor events, alarms, and alerts from devices, and display them. The NM shall alert the operator to problem areas, and provide recommended solutions. The NM shall also store fault history and corrective action inputs, and provide a means to publish status and operational report. The NM shall provide an ability to determine the status of assets via 'drill down' capability to a device's operational parameters or database.

## 4.6 Security Management

The NM shall provide the necessary identification, authentication, integrity, audit and access control capabilities to be accredited under the DITSCAP process. The NM shall plan, monitor, and manage the IA functions described in Section 5.

## 4.7 Accounting Management

The WNW NM shall provide for data logging to support troubleshooting and After Action Reviews.

# Section 5
# Information Assurance

This section states the security requirements for the JTRS WNW. Other security requirements for the JTR Set on which the waveform resides will be addressed separately as part of the radio development. NSA JTR security certification will involve analysis of the WNW instantiated on the JTR, thus the security aspects of the WNW and JTR must complement each other. The WNW security requirements shall be compatible with the SCA Security Supplement and its Security API Appendix. The JTR Set shall provide the cryptographic and TRANSEC keystreams, synchronization, and required cryptographic protection mechanisms. The WNW design shall state the requirements for TRANSEC bitstream and synchronization requirements for COMSEC and TRANSEC.

The WNW instantiated JTR Set supports internal radio functions as well as external wireless network functionality. Refer to the SCA Security Supplement for additional JTRS waveform security information and requirements.

## 5.1 Security Services

### 5.1.1 Confidentiality

The JTRS WNW and associated JTR Set shall provide for NSA Type 1 protection for user data transmitted and shall provide header cover..

### 5.1.2 Availability

The JTRS WNW shall provide the means to recover from loss of cryptographic or TRANSEC synchronization and to resynchronize.

### 5.1.3 Integrity

The JTRS WNW and associated cryptographic functions shall provide anti-spoofing features to assure that user data packets exchanged through wired and wireless networks cannot be maliciously or unintentionally modified.

### 5.1.4 Identification and Authentication

The JTRS WNW shall provide the means to identify and authenticate nodes attempting to join the network. High grade authentication as defined by NSA shall be employed.

The WNW shall employ identification, authentication, authorization and security association mechanisms to support key management functions through wired and wireless networks.

Access controls shall be employed to limit WNW reconfiguration to the appropriate personnel or organizations.

## 5.2 Waveform Security Functions

The JTRS WNW shall provide for the protection of user information and network protocols.

### 5.2.1 Cryptographic Functions

The WNW software profile, as part of waveform instantiation, shall identify required cryptographic algorithm, and mode of operation to the Domain Manager for transfer to the JTR cryptographic subsystem. The specific cryptographic algorithm and modes for the WNW will be specified by the National Security Agency based on specific WNW parameters identified during WNW design (e.g., throughput requirements, error characteristics of the channel, synchronization requirements, threat environment for the WNW, maximum acceptable latency in throughput for cryptographic and TRANSEC subsystems). Type 1 cryptographic algorithm(s) shall be used to protect classified and sensitive user information transmitted through wireless networks.

Required cryptographic functions include encryption and decryption of data, identification and authentication, header cover or protection (may also be provided through readdressing techniques), and TRANSEC key stream generation.

WNW Network Management control information transmitted to the JTR Set shall be encrypted and packet headers shall be covered except when a waiver to do so is provided by the government.

### 5.2.2 TRANSEC Functions

TRANSEC design features (s) shall consider throughput requirements, environment, frequency band (s) of operation, synchronization requirements, and threat. The TRANSEC design should minimize the probability of intercept (LPI) for LPI modes and maximize anti-jam (AJ) capabilities within the envelope of the throughput requirements and spectrum availability. The level of LPI and AJ capabilities should be adaptable to accommodate degradations in the environment.

#### 5.2.2.1 Anti-Jam (AJ) Functions

The WNW AJ feature shall maximize tolerance to malicious and inadvertent signal interference. Adaptable features may be developed to correspond to varying threats. The WNW developer shall calculate achievable AJ margins for the AJ features. The WNW developer shall specify requirements for TRANSEC keystream generation in bits per second, and define the utilization of the bits.

#### 5.2.2.2 Low Probability of Intercept/Detection (LPI/LPD) Functions

The WNW developer shall develop a featureless waveform for LPI/LPD operations. The WNW developer shall estimate the detectability range and processing requirements for interception of the WNW LPI/LPD waveform. The WNW developer shall specify requirements for TRANSEC keystream generation in bits per second, and define the utilization of the bits.

### 5.2.3 Unattended Operation

The JTRS WNW shall provide for unattended operations. Unattended nodes used exclusively as relays shall not require COMSEC keys in order to perform relaying functions.

### 5.2.4 User Data Separation

Each channel instantiation of a WNW waveform shall assume a single level of classification for user information.

### 5.2.5 WNW Security Policy

The WNW software profile shall define applicable host JTR security policies as defined in the SCA Security Supplement. At a minimum, the WNW security policy shall address items such as cryptographic bypass parameters, network access, type separation to support collaborative work environment, and network management

### 5.2.6 JTR Security Certification and Accreditation

The JTR Set with the WNW application software in operation shall be tested per government specifications as part of achieving NSA security certification and DITSCAP accreditation.

### 5.2.7 WNW Download, Configuration and Operation

The WNW shall incorporate software configuration and identification, authentication and integrity parameters consistent with the SCA Security Supplement, that will permit authenticated download and proper instantiation of the waveform into JTR Sets. The WNW design shall include a protocol for the transmission of JTR waveform software files to JTR nodes for storage, download, and instantiation (under manual intervention). The waveform software files shall be source authenticated and integrity checked by the receiving JTR. If the WNW is classified, it shall be delivered in encrypted form, and then decrypted, authenticated and integrity checked and re-encrypted by the receiving JTR.

### 5.2.8 WNW Audit

The JTR WNW shall provide network audit information related to management of wired and wireless network traffic to network management nodes.

### 5.2.9 Radio Fingerprint Masking

Each radio has its own transmission fingerprint, which can be used by enemy forces to identify, locate and exploit specific radios that are related to command operations. This information can be exploited by the enemy for example to concentrate enemy fire, determine movements, and concentrate hostile information attacks on command elements. Techniques shall be implemented in the WNW, such as noise insertion, to mask these transmissions fingerprints that will effectively deny the enemy this information.

## 5.3 Key and Algorithm Management Functions

### 5.3.1 Local Key Management

The JTR Set will perform required functions for EKMS compatible loading, storage, use, authentication, association and management, and zeroization of WNW keying material. The JTR Set will provide an HMI control mechanism to associate the correct keys, network and mission management data to the instantiated WNW.

### 5.3.2 Remote Key Management

#### 5.3.2.1 Over-the-Air Rekey (OTAR)

The WNW vendor shall propose a message format to provide secure key OTAR transmission and reception using a node specific or broadcast format. The OTAR message shall provide for  authentication of the source of the transmission.

#### 5.3.2.2 Over-the-Air Transfer (OTAT)

The WNW vendor shall propose a message format to provide secure key OTAT transmission and reception using a node specific or broadcast format. The OTAT message shall provide for authentication of the source of the transmission.

#### 5.3.2.3 Over-the-Air Zeroize (OTAZ)

The WNW vendor shall propose a message format to provide secure OTAZ transmission using a node (i.e., specific radio address) format. The OTAZ command shall zeroize or disable keys in the target equipment. Verification of the execution of the OTAZ command is desired. The OTAZ message shall provide Type 1 high grade authentication of the source and content of the transmission.

# Appendix A

# Wideband Networking Waveform (WNW) Frequency Spectrum Guidance

## A-1 Introduction

The JTRS WNW shall use RF spectrum that satisfies technical, operational and regulatory requirements for worldwide operation.

## A-2 Radio Spectrum Regulatory Framework

Each nation uses the ITU Radio Regulations[1] as a point of departure for the development national regulations. National spectrum regulatory administrations promulgate additional rules to tailor national RF usage to individual country requirements. U.S. military forces, whether operating in the US or abroad, generally are required to coordinate spectrum usage with national spectrum administrations and adhere to local rules. Within the US, the military service spectrum management offices coordinate with the National Telecommunications and Information Administration (NTIA)[2]. Outside of the US, the responsible Unified-Command Commander in Chief (CINC) coordinates spectrum requirements with host nations following the procedures outlined in ACP-190[3]. Each nation's coordination requirements will vary somewhat. The ERO[4] frequency allocation table illustrates some of the requirements specific to Europe.[5] Within NATO certain military spectrum requirements have been precoordinated and are reflected in the ARFA Handbook and the NATO Joint Civil/Military Frequency Agreement[6]. With respect to these spectrum regulations, the WNW operating frequency range shall include frequency bands allocated to the mobile radio communications service that are authorized for military use. Since the frequency bands satisfying these criteria may vary by region, the WNW and JTR sets shall incorporate adequate flexibility with respect to operating frequency, bandwidth, modulation, and power to address a range of possible host nation restrictions.

## A-3 Spectrum Access

U.S. military forces will use the WNW for mission training, in support of warfighting, and operations other than war such as peace keeping. The WNW and host devices must have adequate access to the RF spectrum for effective worldwide support of these missions. During training and operations other than war, military RF access will be severely constrained by

[1] International Telecommunication Union Radio Regulations, 1998 Edition.

[2] *Manual of Regulations & Procedures for Federal Radio Frequency Management*, US Department of Commerce, National Telecommunications and Information Administration, January 2000 Edition (http://www.ntia.doc.gov/osmhome/redbook/redbook.html).

[3] ACP 190 US SUPP-2, *Coordination and Registration of Frequencies Used by Military Forces on Foreign Soil*, June 1990, CONFIDENTIAL.

[4] European Radiocommunications Office (ERO) of the European Conference of Postal and Telecommunications Administrations (CEPT)

[5] ERO Report 25, *Frequency Range 29.7 MHz to 105 GHz and Associated European Table of Frequency Allocations and Utilisations*, European Radiocommunications Committee, Brugge, Belgium, February 1998 (http://www.ero.dk/doc98/official/pdf/Rep025.pdf).

[6] *NATO Joint Civil/Military Frequency Agreement*, NATO Allied Radio Frequency Agency, 11 November 1994.

national spectrum regulations and the need to avoid interference with the surrounding civilian and local government spectrum users. For political and other reasons, many spectrum use restrictions may remain in effect even in wartime. In all scenarios, WNW devices must also compatibly coexist with a multitude of existing military RF systems. The WNW should possess spectrum access features that comply with regulatory requirements and can operate in realistic RF environments without causing or suffering interference. When waveform performance requirements conflict with spectrum supportability goals, the waveform design should then include features that help to mitigate the possible effects of noncompliance or interference.

## A-3.1 Spectrum Access Features

### A-3.1.1 Variable Bandwidth

A WNW with a variable RF bandwidth is desired to accommodate the range of frequency channel bandwidths that have been established by regulators over the objective JTRS tuning range. Channel plans with associated bandwidth requirements are contained in Reference 2 for many U.S. Government frequency bands. In addition, the Department of Defense (DoD) has established its own plan for the 225-400 MHz band.[7] Waveform features that may be adjusted to provide a variable bandwidth include data rate, coding rate, direct sequence spreading rate, and transmit duty cycle for burst waveforms. Alternatively, a waveform such as non-contiguous orthogonal FDM (OFDM) may be used to divide a wideband data stream into multiple narrowband signals compatible with legacy narrowband channeling and assignment techniques. If the WNW operating frequency range includes either the 29.89-50 MHz or 225-400 MHz sub-bands, the WNW should be capable of satisfying the maximum necessary bandwidth requirements of 40 kHz and 1.2 MHz respectively for these bands (References 2 and 7). These bandwidth requirements apply to contiguous channels. Waveform designs requiring multiple non-contiguous channels (i.e., control & message channels, frequency hopping, or OFDM) may have a total cumulative minimum bandwidth requirement exceeding these limits. Constraints for other frequency ranges and OCONUS areas will vary.

### A-3.1.2 Spectrum Reuse and Efficiency

Since small amounts of spectrum are available to the military for mobile communications below 2 GHz, the WNW must be designed to be spectrum efficient. A Joint Task Force area will require numerous subnets and dedicated spectrum resources cannot be provided for each one. The waveform should facilitate a high rate of reuse, such that unique subnets can occupy the same frequency channels without large geographic separation. TDMA, CDMA, adaptive power management, and smart antennas are examples of established technologies that should be considered for application to this problem.

### A-3.1.3 Access Flexibility

The WNW design should have adequate flexibility to accommodate special spectrum access situations. Often this may involve the use of frequency bands not normally

[7] USMCEB-M-067-99, *Department of Defense Frequency Plan for the 225-400 MHz Band*, 30 June 1999.

available to the U.S. military. Examples include operations in locally unused civilian bands (i.e., television channels) at isolated military test ranges or in overseas areas that have different frequency bands allocated to the military. Consequently, the WNW and host devices should be capable of operation in multiple military and civil frequency bands.

### A-3.1.4 Interference Mitigation

WNW performance requirements such as anti-jamming (AJ) and low probability of intercept (LPI) may result in WNW modes that don't fit well within the current spectrum regulatory framework. Modes using wide RF bandwidth and frequency-hopped waveforms are in this category. Their operation has generally been permitted only under very restrictive conditions tailored to specific operating locations. For these kinds of difficult to accommodate waveforms, the WNW design should allow for adaptive features that enhance the potential for spectrum sharing. This includes sharing with other WNW users as well as legacy waveform users. Effective sharing strategies should maximize WNW spectrum efficiency and facilitate shared use of frequency channels assigned to legacy systems. For example, a WNW radio might scan the spectrum within its tuning range and then dynamically select an optimum transmission frequency, bandwidth, and RF power level intended to minimize interference to itself and the background RF environment. Since specific adaptive algorithms of this type have not yet been approved by spectrum regulators, it is important that the WNW media access control (MAC) be segmented into modular software components that permit the easy insertion of access algorithms approved at a later date for a specific location or mission. Adaptive spectrum access algorithm operation and design should be coordinated with other waveform logic affecting quality of service (QoS).

### A-3.1.5 Access Control

To adapt to local regulatory and EMI constraints, the WNW and associated radio require maximum RF flexibility with regard to frequency range, tuning increment, power, bandwidth, and duty cycle. A high degree of flexibility also requires adequate controls to ensure that only the authorized range of possible values may be used in a particular situation. At least three levels of control should be supported by the WNW design: user/operator, theater, and DoD national. Waveform features common to all applications of the WNW will be controlled at the DoD national level. These features may be embedded in the waveform software logic or specified in the Domain Profile files. Theater-level controls should be provided to specify the subset of waveform capabilities appropriate to certain geographic areas. Authorized frequency bands, frequency hopsets, modes, power levels, and adaptive spectrum access protocols are examples of items appropriate to control at the theater level. The Domain Profile or legacy fill data provide control of these waveform attributes in accordance with directives established for the theater. User/operator control is normally implemented via the human-machine interface (HMI) and allows the operator to select from the range of waveform operations permitted by the DoD national and theater-level controls. For example the user might be able to choose a specific network, frequency channel, or waveform function from a list authorized for the particular theater. These levels of access control are needed to limit WNW reconfiguration to the appropriate personnel or organizations. Authentication checking is needed for software downloads to ensure that radios can only run authorized software. A means of checking the software version and authentication information from the user interface should be provided for audit purposes.

# Appendix B

# WNW Message Performance Requirements

**Table B-1 WNW Data Performance Requirements**

| Priority Level | Message Size (bits) | Message Rate (Messages/min) | | Message Completion Rate (fraction of messages successfully received) | Message Latency (x% of received messaged received within y seconds) | |
|---|---|---|---|---|---|---|
| | | Threshold | Objective | | Threshold | Objective |
| 1 (Flash Override) | 65000 | 35 | 80 | 0.95 | 95% < 5sec | 95% < 1sec |
| | 500000 | 2 | 5 | 0.95 | 95% < 40sec | 95% < 8sec |
| 2 (Flash) | 65000 | 80 | 200 | 0.95 | 95% < 15sec | 95% < 8sec |
| | 500000 | 4 | 10 | 0.95 | 95% < 120sec | 95% < 64sec |
| | 1000000 | 2 | 5 | 0.95 | 95% < 240sec | 95% < 128sec |
| 3 (Immediate) | 65000 | 350 | 900 | 0.9 | 90% < 30sec | 90% < 15sec |
| | 500000 | 15 | 40 | 0.9 | 90% < 240sec | 90% < 120sec |
| | 1000000 | 3 | 10 | 0.9 | 90% < 480sec | 90% < 240sec |
| 4 (Priority) | 95000 | 230 | 575 | 0.9 | 90% < 300sec | 90% < 160sec |
| | 1000000 | 15 | 35 | 0.9 | 90% < 3000sec | 90% < 1600sec |
| | 5000000 | 0.3 | 0.75 | 0.9 | 90% < 14,400sec | 90% < 7680sec |
| 5 (Routine) | 95000 | 230 | 575 | 0.9 | 90% < 600sec | 90% < 320sec |
| | 1000000 | 15 | 35 | 0.9 | 90% < 6300sec | 90% < 3360sec |
| | 5000000 | 0.3 | 0.75 | 0.9 | 90% < 31,500sec | 90% < 16,800sec |

### Table B-2 Multimedia Packet Delivery Requirements

| Priority Level | Real Time Multimedia Traffic Type | Packet performance per radio hop for a multi hop scenario | | | |
|---|---|---|---|---|---|
| | | Threshold | | Objective | |
| | | Maximum Delay | Maximum Packet loss | Maximum Delay | Maximum Packet loss |
| 1 | Tactical Voice | 75ms | 0.5% | 50ms | 0.3% |
| 2 | Tactical Video | 100ms | 0.4% | 80ms | 0.2% |
| 3 | Non-Tactical Voice | 75ms | 0.5% | 50ms | 0.3% |
| 4 | Non-Tactical Video | 100ms | 0.4% | 80ms | 0.2% |
| 5 | Other Multimedia Traffic | 100ms | 0.4% | 80ms | 0.2% |

# Appendix C
# Test Scenario Definition

This appendix defines a group of Test Scenarios as a starting point for determining the performance of the Wideband Networking Waveform. As referenced in the main section of this document these test scenarios will be used to measure network throughput, Join Time, Self Healing Time, the affects of network bifurcation and other requirements as appropriate. The complete test and simulation guidance will be provided in separate documents. The Test and Evaluation Master Plan, WNW Model Development and Performance Guidelines Document, and the Operational Test Scenarios and will be provided by the JTRS Joint Program Office (JPO).

**Test Scenario 1: Point-to-Point**

Figure C-1 illustrates the node configuration for the test scenario 1. The RF Channel is defined as one of four possible channels creating Test Scenarios 1a, 1b, 1c, or 1d. The test measurements are made with the external test equipment as shown in the Figure. The RF Channels are defined as the following;

a) One Propagation Path, no Fading, 145 dB attenuation

b) Two Propagation Path, Slowly Fading Channel defined by
    Path #1: Ricean Fading, Fade Rate $F_d$[8]=1 Hz, 130 dB attenuation
    Path #2: Rayleigh Fading, $T_{1-2}$[9]=0.01 microsecond, $F_d$=10 Hz, $L_{1-2}$[10] =-6 dB

c) Three Propagation Path, Fading Channel defined by
    Path #1: Ricean Fading, $F_d$=10 Hz, 130 dB attenuation
    Path #2: Rayleigh Fading, $T_{1-2}$=0.07 microsecond, $F_d$=10 Hz, $L_{1-2}$=-5 dB
    Path #3: Rayleigh Fading, $T_{1-3}$=0.80 microsecond, $F_d$=10 Hz, $L_{1-3}$=-15 dB

d) Three Propagation Path, Fast Fading Channel defined by
    Path #1: Ricean Fading, $F_d$=25 Hz, 130 dB attenuation
    Path #2: Rayleigh Fading, $T_{1-2}$=0.9 microsecond, $F_d$=25 Hz, $L_{1-2}$=-3 dB
    Path #3: Rayleigh Fading, $T_{1-3}$=5.1 microsecond, $F_d$=25 Hz, $L_{1-3}$=-9 dB

[8] Fade Rate, $F_d$

[9] The Differential Delay is equal to the difference between the propagation time of the first path and the propagation time of the second path ($T_{1-2} = T_1 – T_2$)

[10] The Differential Loss is equal to the difference between the propagation loss associated with the first path and the propagation loss associated with the second path ($L_{1-2} = L_1 – L_2$)

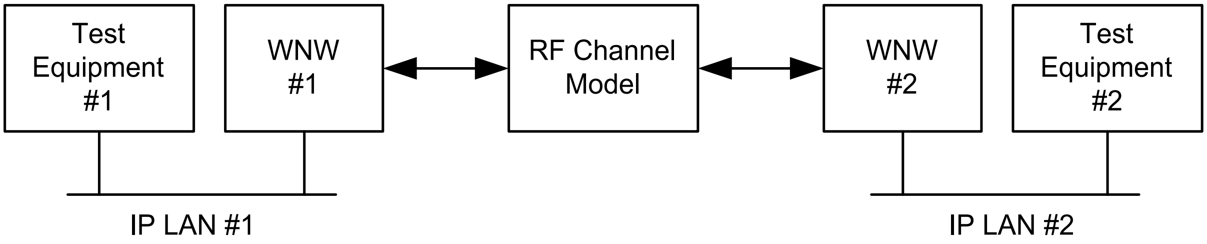

Figure C-1: Test Scenario 1: Point-to-Point

**Test Scenario 2: Point-to-Relay-to-Point**

Figure C-2 illustrates the node configuration for the test scenario 2. The RF Channel is defined as one of four possible channels creating Test Scenarios 2a, 2b, 2c, or 2d. The test measurements are made with the external test equipment as shown in the Figure. The RF Channels are defined in Test Scenario 1.

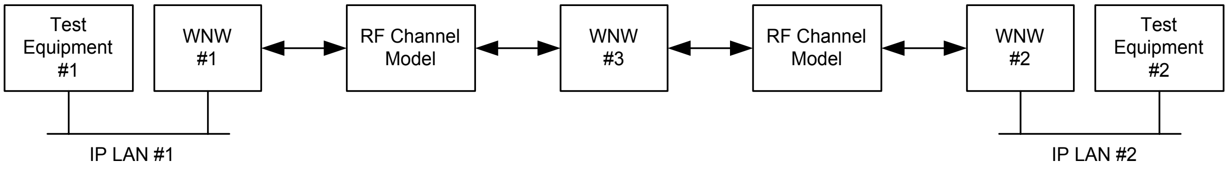

Figure C-2: Test Scenario 2: Point-to-Relay-to-Point

**Test Scenario 3: Seven Node Static Network**

Figure C-3 describes the topology of a seven node static network. Grid spacing represents 3 km. Propagation losses should be computed using the plane-earth model with antennas at 2.4 m above ground level. The message profile will be as defined in Appendix B with every node communicating with every other node in approximately equal measures.

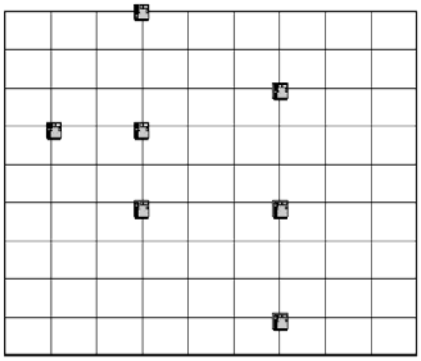

Figure C-3: Test Scenario 3: Seven Node Static Network.

**Test Scenario 4: 100 Node Network.**

Figure C4a shows 100 nodes in a grid formation with approximately equal spacing between the nodes.

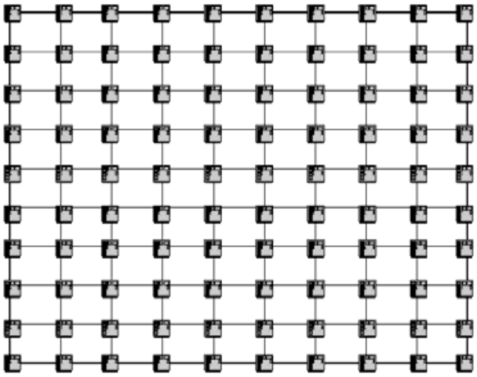

Figure C4a – Test Scenario 4a: 100 Node Scenario

Using the scenario in Figure C4a tests will be performed for dense networks (i.e. when the average number of nodes within transmission distance is greater than 15) and sparse networks (i.e. when the average number of nodes within transmission distance is less than 5).
Tests will also be performed with at least one half of the nodes connected to external routers to test dynamic internetworking. Tests will also be performed with one half of the nodes moving away from the other half to the point of network bifurcation and then the nodes will move back to form a large network.

Figure C4b and C4c show other scenarios based on the 100 node laydown. C4b shows 100 nodes with the node at position 5,5 (measured from top left) elevated to 10000 feet to represent a UAV or air platform. C4c shows the scenario with a UAV and also with 4 nodes moving from the top left to the bottom right of the network at an average speed of approximately 80 kilometers per hour.

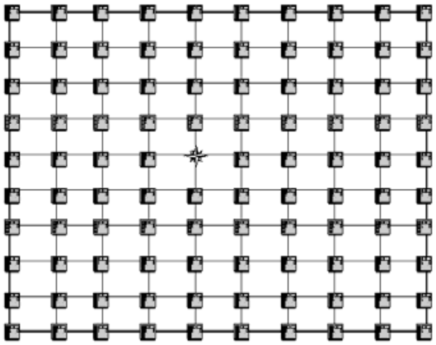

Figure C4b – Test Scenario 4b: 100 nodes with UAV

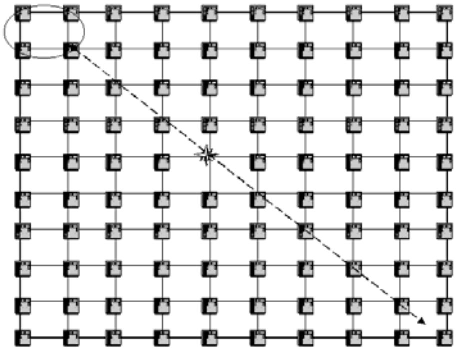

Figure C4c – Test Scenario 4c: 100 nodes with UAV and 4 movers

Traffic Model

Traffic loading will include unicast, multicast, and broadcast traffic. The relative loading percentages of these traffic types will be 50, 25, and 25, respectively, as a baseline with additional tests using different ratios. Fifty multicast groups will be in use with sizes varying from a few nodes to more than half of the nodes with an average group membership of 20 nodes. The message profile will be as defined in Appendix B with every node communicating with every other node in approximately equal measures. Ten concurrent voice circuits can be assumed.

For test analysis purposes the message completion rate for multicast messages will be defined as the total number of multicast messages that were received divided by the total number that should have been received. Data throughput for multicast messages will be defined as the transmit message size multiplied by the number of recipients that correctly received the message. For multicasting of large messages a reliable multicast file transfer protocol can be assumed.

Test Scenario 5: Operationally Representative

The JTRS JPO will define further scenarios based on the operational employments described in section 1 of this document that will supplement the technical test scenarios 1 to 4. The scenarios to be provided by the JTRS JPO will scale to full size deployments as described in section 1 of this document. It is envisaged that these scenarios will initially be used for modeling and simulation during the development of the WNW but will also form that basis of future large scale field trials.

# Appendix D
# Glossary

## PART I – ACRONYMS

| | |
|---|---|
| AAAV | Advanced Amphibious Assault Vehicle |
| ADNS | Automated Digital Network System |
| AEF | Aerospace Expeditionary Force |
| AEW | Aerospace Expeditionary Wing |
| AOE | Fast Combat Support Ship |
| API | Application Programming Interface |
| ARG | Amphibious Readiness Group |
| ATM | Asynchronous Transfer Mode |
| BG | Battle Group |
| BGP | Border Gateway Protocol |
| C2 | Command and Control |
| C4ISR | Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance |
| CG | Cruiser, Guided Missile |
| COC | Combat Operations Center |
| COTS | Commercial Off-the-Shelf |
| CV | Aircraft Carrier |
| CVN | Aircraft Carrier, Nuclear-Powered |
| DD | Destroyer |
| DDG | Destroyer, Guided Missile |
| EMCON | Emission Control |
| FDD | Functional Description Document |
| | First Digitized Division |
| FFG | Frigate, Guided Missile |
| GPS | Global Positioning System |
| HMMWV | High-Mobility Multipurpose Wheeled Vehicle |
| IGMP | Internet Group Management Protocol |
| ISNS | Integrated Shipboard Network System |
| ISR | Intelligence, Surveillance, and Reconnaissance |

| | |
|---|---|
| JMCOMS | Joint Maritime Communications Strategy |
| JTRS | Joint Tactical Radio System |
| LAN | Local Area Network |
| LHA | Amphibious Assault Ship |
| LHD | Amphibious Assault Ship (Second Generation) |
| LPD | Landing Platform Dock |
| | Low Probability of Detection |
| LPI | Low Probability of Intercept |
| LSD | Landing Ship, Dock |
| MAGTF | Marine Air-Ground Task Force |
| MEF | Marine Expeditionary Force |
| MEU | Marine Expeditionary Unit |
| MOSPF | Multicast extension to Open Shortest Path First |
| M-PNNI | Mobility extensions to Private Network to Network Interface |
| NDI | Non-Developmental Item |
| NTDR | Near Term Digital Radio |
| OMFTS | Operational Maneuver from the Sea |
| OSI | Open Systems Interconnect |
| OSPF | Open Shortest Path First |
| PIM | Protocol Independent Multicast |
| PNNI | Private Network to Network Interface |
| QoS | Quality of Service |
| RF | Radio Frequency |
| SATCOM | Satellite Communications |
| SCA | Software Communications Architecture |
| SINCGARS | Single Channel Ground Air Radio System |
| Sink | Terminating or receiving node or subscriber |
| Source | Originating or transmitting node or subscriber |
| SSN | Ship, Submersible, Nuclear-Powered |
| STOM | Ship-to-Objective Maneuver |
| TI | Tactical Internet |
| TOC | Tactical Operations Center |
| TRANSEC | Transmission Security |

| | |
|---|---|
| UAV | Unmanned Air Vehicle |
| VTUAV | Vertical Takeoff Unmanned Aerial Vehicle |
| WAN | Wide Area Network |
| WLAN | Wireless Local Area Network |
| WNW | Wideband Networking Waveform |

## PART II – Terms and Definitions[11]

Communication. Communication is information transfer, among users or processes, according to agreed conventions.

Compatibility. Capability of two or more items or components of equipment to exist or function in the same system or environment without mutual interference.

Data Rates. The aggregate rates at which data pass a point in the transmission path of a system. LOW, MEDIUM and HIGH Data rates are further defined in applicable MIL STDs for applicable waveform and system usages.

Gateway. A gateway in a communications network is a network node equipped for interfacing with another network that uses different protocols. A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires that mutually acceptable administrative procedures be established between the two networks. A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions.
*A multi-channel JTR set includes inter-network gateway services between its channels or networks.*

Information Assurance. Information Operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.

Integrity. Integrity is the property that data, systems, services, and other controlled resources have not been altered or destroyed in an unauthorized manner. It is the quality of an information system (IS) that reflects the logical correctness and reliability of the operating systems and the logical completeness of the hardware and software that implement the protection mechanisms.

Inter-Networking. Inter-networking is the process of inter-connecting two or more individual networks to facilitate communications between nodes of the inter-connected networks. Each network may be distinct, with its own addresses, internal protocols, access methods, and

[11] Many of these definitions are reprinted from the JTRS ORD 30 Jan 2001 for convenience.

administration. *Individual networks connected to form a JTR* i*nter-network will share the same general operating mode, i.e. voice, data, or video.*

Inter-Operability. Inter-operability is the condition achieved among communications-electronics systems or items of equipment when information or services can be exchanged directly and satisfactorily between them and their users. *For example, interoperability could be established between a SINCGARS voice net and another system voice net through a transparent interface of a JTR set operating simultaneously in both nets.*

JTR Set. A JTR set is integrated on a user's platform as a completely functional configuration of radio communications hardware and software that provides the full range of JTR System services required by the user system. The JTR Set may include one or more operating components. A JTR set does not include the user's host system computer, but does provide all aspects of radio communications and network services intended for the user's host system. A JTR set includes, but is not limited to such items as receiver-transmitters; microphones and speakers, antennae; power amplifiers; batteries for dismounted sets; interconnecting cables; platform installation kits, routers and other networking components; etc. *JTR set examples:*
*Set 1. Hand-held 1-channel/1 mode HF voice radio, power, and antenna.*
*Set 2. Hand-held 1-channel/1 mode VHF voice radio, power, and antenna.*
*Set 3. Dismounted 2-channels/2modes VHF voice/VHF data radio, power, and antenna.*
*Set 4. Vehicular or Aviation 3-channels/2modes VHF voice/VHF data/UHF/data radio, inter-networking components, power, antenna, platform installation kit, etc.*
*Set 5. A 6 channels/2modes JTR Set, designed for interim use during the transition from legacy radios to JTR Set, could be comprised of 1 software-defined radio programmed for 3 channels (e.g. SINCGARS voice net 1, SINCGARS voice net 2, and HAVEQUICK voice net); 3 adjunct legacy radios (e.g. JTIDS, EPLRS and UHF DAMA/DASA); and the means to inter-connect the channels as required for inter-networking.*

JTR System (JTRS). JTR System is a generic reference to the system that encompasses the aggregate of all aspects and components (including JTR Sets) that constitute and enable the installation, operation, and maintenance of the JTR System communications architecture. Unless explicitly stated otherwise, in this ORD JTRS is a collective term that refers to the entire system.

Latency. Latency is a quality or state of being that is marked by suspension of activity, or delay, in performing an operation. In an information transfer operation; latency is a measure of the time that elapses at various stages of the transfer. *The information latency that is attributable to the communications means is the elapsed time from when a user terminal submits information to the means until the information is submitted to the intended user terminal. Ideally, information will flow across the JTR* System *networks with near-zero latency.*

Network. A network is an inter-connection of three or more communicating entities.

Network Administration. Network administration is a group of network management functions that provide support services; ensure that the network is used efficiently; and ensure that prescribed service quality objectives are met. Network administration may include activities such as network address assignment, assignment of routing protocols and routing table configuration, and directory service configuration.

Network Architecture. Network architecture is the design principles, physical configuration, functional organization, operational procedures, and data formats used as the basis for the design, construction, modification, and operation of a communications network.

Network Bridge. A network bridge is a device that links or routes signals from one network to another

Network Interface. Network interface is the point of interconnection between a user terminal and a network or between one network and another network. *The JTR Sets will provide the means for interface of user terminals to individual networks (e.g. EPLRS, SINCGARS) and between networks (e.g. between EPLRS and SINCGARS data networks).*

Network Management. Network management is execution of a set of functions required for controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a telecommunication network. Network management includes performing functions such as initial network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, and accounting management. Network management does not usually include management of user terminal equipment (See also System Management).

Network Throughput. Network Throughput is defined as the aggregate User Throughput of all WNW nodes in the network.

Network User. A person, organization, or system that employs the services provided by a telecommunication network for transfer of user information.

Node. A general term used to describe either a terminal connection point common to two or more branches of a network; a switch forming a network backbone; patching and control facilities; technical control facilities.

Protocol. A protocol is a formal set of conventions governing the format and control of interaction among communicating functional units. In layered communications system architecture, a protocol is a formal set of procedures that are adopted to facilitate functional inter-operation within the layered hierarchy.

Radio Channel. A radio channel is an assigned band of frequencies sufficient for radio communication. The bandwidth needed for a radio channel depends upon the type of transmission and the frequency tolerance.

Radio Net. An organization of radio sets directly communicating on a common channel or frequency.

Radio Network. An interconnection of three or more radio sets communicating with each other, but not necessarily on the same channel or frequency *(e.g. a multi-channel network that may choose one or more available channels for a communications session between its nodes).*

Route and Retransmission. (Previously stated as Cross-banding) To route and retransmit is the capability to automatically pass user information from a channel operating on one frequency band to a channel operating on another frequency band. Within a multi-channel radio set, routing and retransmission may occur between any input channel and any output channel that the set operates using the same mode of operation (voice, data, or video). Within a network, information may flow between two nodes that do not share a common channel by routing the data through a multi-channel node that operates on both channels used by the source and destination nodes. *For example, in a JTR set operating the data mode simultaneously in two SINCGARS data nets and one EPLRS net, routing and retransmission of data flow can be accomplished between source nodes of one net and destination nodes of one or both other nets. Routing and retransmission in the JTR System may include use of multi-link operations*.

Three Tiered Communication Architecture. Each of the service's communication architectures can be broken down into three primary tiers of communication links. The lowest level is Tier 1 which refers to the edges of the network and normally consist of stub networks that can either be single subnets or small Internets and are not required to relay non local traffic. Tier 2 refers to the primary mission of the WNW providing a communications backbone to the Tier 1 networks and support the relay of transit as well as relay traffic. Tier 3 refers to external networks that are not a part of the WNW that suppor transit and local traffic. These include trunk networks, satellite communications and other radio networks. Tiers 2 and 3 connect together at several points to provide an adaptable internetwork that appears seamless to the user.

Transmission Security (TRANSEC). A component of COMSEC resulting from the application of measures taken to protect transmissions from interception and exploitation by means other than cryptanalysis (Cryptanalysis is defined as "Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and /or key employed in the encryption.). Transmission security is the protection of the communications paths against attack. Defensive measures include anti-jam, low probability of detection, low probability of intercept, spread spectrum techniques such as frequency hopping and direct sequence spreading, and protected distribution.

Type 1: A type 1 product is a classified or controlled cryptographic item endorsed by NSA for securing classified and sensitive U.S. Government information, when appropriately keyed. The term refers only to products, and not to information, key, services or controls. Type 1 products contain classified NSA algorithms. They are available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulation.

User Throughput. Defined as the amount of user application layer information successfully transferred from the source to the sink in unit time. For test purposes this can be assumed to be for directly attached hosts using off the shelf protocols

Wide-Band. A wide band circuit may have a bandwidth wider than normal for the type of circuit, frequency of operation, or type of modulation. *In common usage, "wide-band" refers to a high capacity for information transfer. In JTR System usage, wide-band refers to a networked radio waveform that has a node-to-node capacity for information transfer of 512 Kbps or greater.*

Waveform. A waveform is the representation of a signal as a plot of amplitude versus time. *In general usage, the term waveform refers to a known set of characteristics, e.g. SINCGARS or EPLRS "waveforms". In JTR System usage, the term waveform is used to describe the entire set of radio functions that occur from the user input to the RF output and vice versa. A JTR System "waveform" is implemented as a re-useable, portable, executable software application that is independent of the JTR System operating system, middleware, and hardware.*

# Appendix E
# JTRS WNW FDD TRACEABILITY MATRIX

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 1 | The JTRS WNW network shall provide connectivity in an operational area through self-forming, self-healing mobile ad hoc networking. | | | |
| FDD 2 | The JTRS WNW network shall support worldwide connectivity by inter-networking with IP-based networks on other media. | | | |
| FDD 3 | The JTRS WNW shall support both backbone links (tier 2) and subnet links (tier 1) as described in Section 1 and defined in Appendix D Part II – Terms and Definitions. | | | |
| FDD 4 | The JTRS WNW shall have parameters and functions that support special operating modes  specified in paragraphs 2.2.1 through 2.2.5. | | | |
| FDD 5 | The JTRS WNW shall automatically perform a gateway function between the backbone links (Tier 2) and the subnet links (Tier 1). | | | |
| FDD 6 | The gateway function shall include communications between the WNW network and nodes operating in the Asymmetric Networking Mode and the LPI/LPD Networking Mode. | | | |
| FDD 7 | The JTRS WNW shall automatically perform asymmetric transmission rates between JTRS WNW nodes. | | | |
| FDD 8 | Data packet transmission between different nodes shall be optimized on a packet by packet basis to support various RF channel conditions. | | | |
| FDD 9 | The JTRS WNW shall support a receive-only (radio silent) operation function at one or more nodes that require emission control (EMCON). | | | |
| FDD 10 | The receive-only function shall be initiated when operationally required by the network control manager or the JTRS operator. | | | |
| FDD 11 | A JTRS WNW node operating in this mode shall not transmit any RF information on the network. | | | |
| FDD 12 | The JTRS WNW shall facilitate smooth transition to and from the receive-only and normal operations. | | | |
| FDD 13 | The JTRS WNW shall continue to forward data to any host or any router attached to the JTR Set. | | | |

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 14 | A JTRS WNW node operating under covert conditions shall be capable of joining and participating in the WNW network using a low probability of intercept/low probability of detection (LPI/LPD) function. | | | |
| FDD 15 | The LPI/LPD function shall be initiated when operationally required by the network control manager or the JTRS operator. | | | |
| FDD 16 | In this mode of operation, the node shall perform the network control handshaking/signaling that is necessary to join the network. | | | |
| FDD 17 | This LPI/LPD node shall have minimal impact on the data rate of the WNW network nodes on the backbone of the WNW network that are not operating in LPI/LPD mode. | | | |
| FDD 18 | The JTRS WNW shall support a point-to-point operation mode that optimizes the throughput and latency between two nodes. | | | |
| FDD 19 | The performance of the waveform shall be sufficient to support the operational scenarios described in section 1 using the Message Performance Requirements in Appendix B. | | | |
| FDD 20 | Appendix C provides additional test scenarios that shall be used to verify performance. | | | |
| FDD 21 | The JTRS WNW shall be capable of automatically adaptable data rates. | | | |
| FDD 22 | The JTRS WNW shall provide negotiated automatic fallback to lower data rates for degraded channel conditions or restricted modes of operation. | | | |
| FDD 23 | Conversely, the JTRS WNW shall provide negotiated automatic step-up in data rates for improved channel conditions, to and from each node. | | | |
| FDD 24 | The JTRS WNW shall support user throughputs greater than 5 Mbps in Test Scenario 1a, 1b, 1c and 1d described in Appendix C. | | | |
| FDD 25 | The JTRS WNW shall support user throughputs greater than 2 Mbps in Test Scenario 2a, 2b, 2c and 2d described in Appendix C. | | | |
| FDD 26 | Using Test Scenarios 3 through 5 specified in Appendix C and the message performance requirements in Appendix B the WNW shall support greater than 2 Mbits per second of Network Throughput as a threshold. | | | |

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 27 | The WNW shall have the ability to make efficient use of extra frequency spectrum when available and shall support Network Throughputs of greater than 5 Mbits per second as an objective. | | | |
| FDD 28 | The JTRS WNW operating in the Point-to-Point mode shall support a user throughput rate of greater than 2 Mbps in each direction. | | | |
| FDD 29 | When using antennas and power levels suitable for the respective host platforms, the JTRS WNW line-of-sight point-to-point range shall meet the following requirements:<br>Air-to-Air* at least 370 km (200 nmi)<br>Air-to-Ground/Surface* at least 370 km (200nmi)<br>Ground-to-Ground at least 10 km (5.4 nmi)<br>Ship-to-Ship at least 28 km (15 nmi)<br>Ship-to-Shore at least 28 km (15 nmi) | | | |
| FDD 30 | The JTRS WNW shall provide a packet error rate of less than 0.1% in a back-to-back laboratory configuration with receive signal levels between –100 dBm to –10 dBm. | | | |
| FDD 31 | Tests shall be measured with packet sizes of 64 bytes, 576 bytes and 1500 bytes in Test Scenarios 1a, 1b, 1c, 1d, 2a, 2b, 2c, and 2d described in Appendix C. | | | |
| FDD 32 | The JTRS WNW shall automatically control power to reduce the amount of interference and allow for frequency reuse. | | | |
| FDD 33 | The JTRS WNW shall be able to operate in all tactical RF propagation environments such as hilly, mountainous, dense vegetation, desert, and urban terrain. | | | |
| FDD 34 | The JTRS WNW shall be robust and adaptable to support connectivity during rapidly changing distances and orientations between nodes. | | | |
| FDD 35 | The JTRS WNW shall adapt to the presence of Doppler effects, fading, multipath, and other RF channel conditions in the operating environments and host platform operating profiles. | | | |
| FDD 36 | The JTRS WNW shall use RF spectrum that satisfies technical, operational, and regulatory requirements for worldwide operation. | | | |

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 37 | The WNW operating frequency range shall include frequency sub-bands allocated to the mobile radio communications service that are authorized for military use. | | | |
| FDD 38 | Since the frequency bands satisfying these criteria may vary by region, the WNW and host JTR Sets shall incorporate adequate flexibility with respect to operating frequency, bandwidth, modulation, and power to address a range of possible host nation restrictions. | | | |
| FDD 39 | The JTRS WNW shall be able to operate in tactical RF propagation environments. | | | |
| FDD 40 | The JTRS WNW shall be able to operate in co-site environments typical of C2, ISR, and other communications-intensive platforms (both airborne and surface) as well as within line-of-sight of other wireless/radio networks, radar, and navigation systems. | | | |
| FDD 41 | The JTRS WNW shall include an anti-jam (AJ) feature of operation for protection to prevent the enemy disruption of services. | | | |
| FDD 45 | The WNW shall provide self-organizing, self-healing networks capable of responding to dynamic changes in connectivity. | | | |
| FDD 46 | The WNW network shall provide routing and management protocols/schemes that can rapidly respond to ad hoc changes in network topology caused by such things as node addition and deletion, node movements, antenna shadowing or orientation, terrain masking, or interference. | | | |
| FDD 48 | The performance of the waveform shall be sufficient to support the operational scenarios described in section 1 using the Information Exchange Requirements in Appendix B. | | | |
| FDD 49 | Appendix C provides additional test scenarios that shall be used to verify performance. | | | |
| FDD 50 | The WNW network shall still be able to operate if GPS timing is not available. | | | |
| FDD 51 | The WNW network shall have the capability to integrate an initial network of 150 nodes spread over the operational area into a single network within 15 minutes of system initialization. | | | |

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 52 | The WNW network shall have the capability to automatically add one node to an existing network in less than one minute of the node's request to join the network. | | | |
| FDD 53 | The WNW network shall integrate any node operating in the area of operation into the network. | | | |
| FDD 54 | The WNW network shall support routing and management protocols/schemes that can rapidly respond, without excessive overhead, to ad hoc changes in network topology caused by such things as node addition and deletion, node movements relative to other surface or airborne nodes, antenna shadowing, terrain masking, or interference. | | | |
| FDD 55 | For these ad hoc changes, the WNW network shall provide efficient use of resources while providing adequate performance and without undue organizational or hierarchical restrictions. | | | |
| FDD 56 | The WNW network shall also support network reorganizations introduced through the network management interface within the times shown in Table 3.1.1. | | | |
| FDD 57 | For nodes in Receive-only mode, these routing and management protocols/schemes shall not permit routing through these nodes, nor will they respond to route discovery or other network control queries. | | | |
| FDD 58 | The WNW network shall provide traffic rerouting with minimal loss of packets after a change in network topology (e.g., loss of a node or link). | | | |
| FDD 59 | The JTRS WNW network design shall support connectivity to and between ground or surface mobile platforms moving at speeds relative to other platforms in excess of 120 mph while maintaining network connectivity and traffic transmission integrity. | | | |
| FDD 60 | The JTRS WNW network design shall support network connectivity and traffic transmission integrity to and between airborne platforms for speeds relative to other platforms up to 900 knots at altitudes of tens of feet to over 65,000 feet above sea level. | | | |
| FDD 61 | The JTRS WNW network design shall also support connectivity to and between airborne and ground nodes at relative speeds up to 900 knots. | | | |

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 62 | The WNW shall maintain stated performance when up to 50% of nodes, limited to a maximum of 75 in any network, are moving at the maximum speeds identified above and a further 50% of all nodes are traveling at speeds up to 80 kilometers per hour. | | | |
| FDD 63 | The WNW network shall support protocol suites capable of providing the network service requirements below. | | | |
| FDD 64 | These network services shall operate simultaneously. | | | |
| FDD 65 | The WNW shall support Quality of Service (QoS) mechanisms to support differential handling of traffic classes according to their service requirements. | | | |
| FDD 66 | The mechanisms shall include precedence handling that discriminates among traffic based on its mission importance. | | | |
| FDD 67 | At a minimum, the WNW shall support both DiffServ(RFC 2474) and IP Precedence (RFC 791). | | | |
| FDD 68 | The WNW shall provide preferential treatment of user traffic, with respect to both delivery priority and drop priority. | | | |
| FDD 69 | Military communications traffic will vary in requirements for delay and reliability of delivery; the WNW network shall provide mechanisms appropriate to support these various delivery requirements. | | | |
| FDD 70 | Listed in Appendix B are the five levels of traffic precedence used in the Defense Switched Network.. At a minimum, the JTRS WNW shall provide support for an analogous service. | | | |
| FDD 71 | The WNW shall support QoS mechanisms to ensure optimum performance for multimedia traffic, including data, voice, and video. | | | |
| FDD 72 | In addition to the message latencies and completion rates contained in Table B-1 of Appendix B for data, the WNW network shall satisfy the packet delay and completion rate requirements for multimedia packets in Table B-2 of Appendix B. | | | |
| FDD 73 | The WNW link layer shall support broadcast, multicast, and unicast messages. | | | |

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 74 | The WNW link layer shall provide channel access schemes which:<br>a) Manage access from multiple nodes that are in line of sight of each other;<br>b) Minimize packet collisions between these nodes or at nodes in line of sight of two transmitting nodes which are not in line of sight (“hidden node” problem);<br>c) Maximize simultaneous transmission to receivers that are not in line of sight of each other (“exposed node” problem);<br>d) Provide fair access between nodes transmitting data with the same precedence in the network. | | | |
| FDD 75 | The WNW shall provide standard link layer addressing and messaging schemes that support unicast, multicast, and broadcast transmissions between nodes in line of sight. | | | |
| FDD 76 | The WNW link layer shall provide packet delivery schemes that support assured (acknowledged) and best effort (unacknowledged) message delivery. | | | |
| FDD 77 | The WNW network shall use Internet Protocol addressing schemes, including support for subnet addressing and unique and group addresses | | | |

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 78 | The WNW network shall use routing protocols/schemes that support:<br>a) Unicast, multicast, and broadcast transmissions to nodes or users on any part of the WNW network, or on other military or commercial networks;<br>b) Scalable networks of from 2 to 1,630 nodes which may be densely or sparsely distributed across an operational area;<br>c) Ad hoc changes in network topologies caused by such things as node addition and deletion, node movements, antenna shadowing, terrain masking, or interference without overwhelming the network with routing overhead information;<br>d) Nodes with varying functionality/modes Route transit as well as local traffic. | | | |
| FDD 79 | The WNW shall employ link management schemes that quickly adapt, without excessive overhead, to rapidly varying connectivity status caused by the mobility of each node relative to other ground or airborne nodes. | | | |
| FDD 80 | The JTRS WNW network shall support internetworking between WNW networks and IP-based networks on other media (including terrestrial media, wideband SATCOM, and host platform LANs) to support communication with command authorities, out-of-theater sources of information and support, other in-theater networks, or en-route platforms. | | | |
| FDD 81 | The WNW shall interface with external networks running standard Internet Protocols, including but not limited to IEEE 802.3, Open Shortest Path First (OSPF), Border Gateway Protocol (BGP) V4, Multicast extension to OSPF (MOSPF), Protocol Independent Multicast (PIM) (sparse mode and dense mode), or Internet Group Management Protocol (IGMP). | | | |

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 82 | Any WNW network node interfacing to other military or commercial IP-based networks shall be configurable as an OSPF Area Border Router or Autonomous System Boundary Router. | | | |
| FDD 83 | When the WNW network fragments (healing through WNW links not possible) and the fragments can be healed through external links (tier 3), the WNW shall support communication between hosts attached to different fragments for both IP unicast and IP multicast data. | | | |
| FDD 84 | If a tier 3 network fragments (healing through tier 3 links not possible) and the fragments can be healed through the WNW then the WNW shall support communication between hosts attached to the fragments of the tier 3 network for both IP unicast and multicast data. | | | |
| FDD 85 | The WNW network shall dynamically manage itself, permitting members to join and leave the network without manual intervention, and autonomously execute network security features in section 5. | | | |
| FDD 86 | The WNW network shall also permit a Network Manager to plan, monitor, and manage the JTRS WNW network or to manually intervene for disaster recovery such as to excise unauthorized or compromised JTRS WNW network members and to have operational control for Over the Air Rekeying (OTAR) of COMSEC, TRANSEC, and other security variables. | | | |
| FDD 87 | The WNW Network Manager shall distribute node configuration data from the Network Manager to the appropriate radios. | | | |
| FDD 88 | The WNW shall include functionality sufficient to organize, manage, and dynamically control network connectivity structures, routing mechanisms, bandwidth allocations and spectrum restrictions. | | | |
| FDD 89 | The WNW shall also provide information to and be interoperable with joint network management tools, to allow network managers to remotely identify and configure user access and profile parameters to prioritize users, network access and message delivery. | | | |
| FDD 90 | The JTRS WNW Network Manager shall be DII COE level 6 compliant. | | | |

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 91 | The JTRS WNW and associated network manager shall also comply with the Joint Technical Architecture for network management protocols, and should provide interfaces to COTS standards that meet objective functionality, such as Simple Network Management Protocol Version 3 and Common Open Policy Server Protocol. | | | |
| FDD 92 | WNW Network management software shall be modular in design to aid maintainability, reuse, and tailoring use of the network management application package as required by particular users | | | |
| FDD 93 | The JTRS WNW Network Manager shall exchange management information including, but not limited to, the information exchange requirements listed in Appendix F. | | | |
| FDD 94 | The JTRS WNW network shall provide a Network Management (NM) interface to DOD network management tools and processes to plan the WNW network configuration parameters, monitor the network and permit a Network Manager to make real time parameter changes (e.g. to ensure operations only on authorized frequencies, etc.) from anywhere in the battlefield to optimize network performance. | | | |
| FDD 95 | This interface shall consist of a Graphic User Interface (GUI) that provides interoperability to current and proposed network management environments used within the Joint networking arena (e.g., | | | |
| FDD 96 | The Human Computer Interface (HCI) of the JTRS WNW NM interface shall be in compliance with the Department of Defense (DOD) Technical Architecture Framework for Information Management (Vol. | | | |
| FDD 97 | The WNW NM GUI shall allow access to network member's operational parameters or database as needed; but unauthorized access shall be denied. | | | |
| FDD 98 | The WNW NM GUI shall provide network configuration information such as location of network devices and maintaining information on how devices or objects are configured. | | | |
| FDD 99 | It shall display a physical representation of the network. | | | |

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 100 | The NMT shall be capable of overlaying all network nodes on a map background of the Area of Responsibility using approved symbology in accordance with the JTF Symbol Set. | | | |
| FDD 101 | The map background shall use the Military Grid Reference System and Latitude/Longitude, but not simultaneously. | | | |
| FDD 102 | This display capability shall allow the network manager to use a map background for planning purposes such as profiling radio links, and allow the network manager the capability to disable the map background once the network is engineered to obtain a logical view of the network. | | | |
| FDD 103 | The WNW NM shall provide the capability to view selective groups of nodes or zoom into an area of the network. | | | |
| FDD 104 | The WNW NM shall also provide the capability to collect and save the JTRS WNW network traffic statistics. | | | |
| FDD 105 | Threshold and performance information shall include parameters for intra-network as well as external interfaces. | | | |
| FDD 106 | The WNW NM shall use service defined Common Hardware Software (CHS). | | | |
| FDD 107 | The WNW NM shall provide capabilities to assist the network planning process. | | | |
| FDD 108 | The NM shall have a system level menu that allows the planner to logically progress through the planning process. | | | |
| FDD 109 | The NM shall automatically perform the analysis of the propagation loss on the transmission systems and provide feedback, visual and/or hardcopy, to the planner. | | | |
| FDD 110 | Planner shall be capable of importing text and graphics files created by other office automation applications as necessary to produce network plans and configuration files. | | | |
| FDD 111 | The WNW NM shall be able to reconfigure radios during the mission to reflect changing mission requirements. | | | |
| FDD 112 | The Network Manager shall monitor and manage the JTRS wideband network using the WNW NM GUI. | | | |

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 113 | The WNW NM shall display the nodes of the network and their configuration and operating performance data. | | | |
| FDD 114 | The WNW NM shall identify and process events and reported faults. | | | |
| FDD 115 | The WNW NM shall provide a fault management capability to detect and alert the user to problem areas, identify and diagnose problems in performance and configuration, provide recommended solutions, and manage and track faults until they are successfully corrected. | | | |
| FDD 116 | The WNW NM shall monitor the status of the radios by acquiring and displaying radio performance data. | | | |
| FDD 117 | It shall monitor network condition, report changes in status, and respond to evolving network changes. | | | |
| FDD 118 | The NM shall receive input from devices to obtain utilization and status, monitor events, alarms, and alerts from devices, and display them. | | | |
| FDD 119 | The NM shall alert the operator to problem areas, and provide recommended solutions. | | | |
| FDD 120 | The NM shall also store fault history and corrective action inputs, and provide a means to publish status and operational report. | | | |
| FDD 121 | The NM shall provide an ability to determine the status of assets via ‘drill down’ capability to a device’s operational parameters or database. | | | |
| FDD 122 | The NM shall provide the necessary identification, authentication, integrity, audit and access control capabilities to be accredited under the DITSCAP process. | | | |
| FDD 123 | The NM shall plan, monitor, and manage the IA functions described in Section 5. | | | |
| FDD 124 | The WNW NM shall provide for data logging to support troubleshooting and After Action Reviews. | | | |
| FDD 125 | The WNW security requirements shall be compatible with the SCA Security Supplement and its Security API Appendix. | | | |
| FDD 126 | The JTR Set shall provide the cryptographic and TRANSEC keystreams, synchronization, and required cryptographic protection mechanisms. | | | |

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 127 | The WNW design shall state the requirements for TRANSEC bitstream and synchronization requirements for COMSEC and TRANSEC. | | | |
| FDD 128 | The JTRS WNW and associated JTR Set shall provide for NSA Type 1 protection for user data transmitted and shall provide header cover.. | | | |
| FDD 129 | The JTRS WNW shall provide the means to recover from loss of cryptographic or TRANSEC synchronization and to resynchronize. | | | |
| FDD 130 | The JTRS WNW and associated cryptographic functions shall provide anti-spoofing features to assure that user data packets exchanged through wired and wireless networks cannot be maliciously or unintentionally modified. | | | |
| FDD 131 | The JTRS WNW shall provide the means to identify and authenticate nodes attempting to join the network. | | | |
| FDD 132 | High grade authentication as defined by NSA shall be employed. | | | |
| FDD 133 | The WNW shall employ identification, authentication, authorization and security association mechanisms to support key management functions through wired and wireless networks. | | | |
| FDD 134 | Access controls shall be employed to limit WNW reconfiguration to the appropriate personnel or organizations. | | | |
| FDD 135 | The JTRS WNW shall provide for the protection of user information and network protocols. | | | |
| FDD 136 | The WNW software profile, as part of waveform instantiation, shall identify required cryptographic algorithm, and mode of operation to the Domain Manager for transfer to the JTR cryptographic subsystem. | | | |
| FDD 137 | Type 1 cryptographic algorithm(s) shall be used to protect classified and sensitive user information transmitted through wireless networks. | | | |
| FDD 138 | WNW Network Management control information transmitted to the JTR Set shall be encrypted and packet headers shall be covered except when a waiver to do so is provided by the government. | | | |
| FDD 139 | TRANSEC design features (s) shall consider throughput requirements, environment, frequency band (s) of operation, synchronization requirements, and threat. | | | |

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 140 | The WNW AJ feature shall maximize tolerance to malicious and inadvertent signal interference. | | | |
| FDD 141 | The WNW developer shall calculate achievable AJ margins for the AJ features. | | | |
| FDD 142 | The WNW developer shall specify requirements for TRANSEC keystream generation in bits per second, and define the utilization of the bits. | | | |
| FDD 143 | The WNW developer shall develop a featureless waveform for LPI/LPD operations. | | | |
| FDD 144 | The WNW developer shall estimate the detectability range and processing requirements for interception of the WNW LPI/LPD waveform. | | | |
| FDD 145 | The WNW developer shall specify requirements for TRANSEC keystream generation in bits per second, and define the utilization of the bits. | | | |
| FDD 146 | The JTRS WNW shall provide for unattended operations. | | | |
| FDD 147 | Unattended nodes used exclusively as relays shall not require COMSEC keys in order to perform relaying functions. | | | |
| FDD 148 | Each channel instantiation of a WNW waveform shall assume a single level of classification for user information. | | | |
| FDD 149 | The WNW software profile shall define applicable host JTR security policies as defined in the SCA Security Supplement. | | | |
| FDD 150 | At a minimum, the WNW security policy shall address items such as cryptographic bypass parameters, network access, type separation to support collaborative work environment, and network management | | | |
| FDD 151 | The JTR Set with the WNW application software in operation shall be tested per government specifications as part of achieving NSA security certification and DITSCAP accreditation. | | | |
| FDD 152 | The WNW shall incorporate software configuration and identification, authentication and integrity parameters consistent with the SCA Security Supplement, that will permit authenticated download and proper instantiation of the waveform into JTR Sets. | | | |

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 153 | The WNW design shall include a protocol for the transmission of JTR waveform software files to JTR nodes for storage, download, and instantiation (under manual intervention). | | | |
| FDD 154 | The waveform software files shall be source authenticated and integrity checked by the receiving JTR. | | | |
| FDD 155 | If the WNW is classified, it shall be delivered in encrypted form, and then decrypted, authenticated and integrity checked and re-encrypted by the receiving JTR. | | | |
| FDD 156 | The JTR WNW shall provide network audit information related to management of wired and wireless network traffic to network management nodes. | | | |
| FDD 157 | Techniques shall be implemented in the WNW, such as noise insertion, to mask these transmissions fingerprints that will effectively deny the enemy this information. | | | |
| FDD 158 | The WNW vendor shall propose a message format to provide secure key OTAR transmission and reception using a node specific or broadcast format. | | | |
| FDD 159 | The OTAR message shall provide for  authentication of the source of the transmission. | | | |
| FDD 160 | The WNW vendor shall propose a message format to provide secure key OTAT transmission and reception using a node specific or broadcast format. | | | |
| FDD 161 | The OTAT message shall provide for authentication of the source of the transmission. | | | |
| FDD 162 | The WNW vendor shall propose a message format to provide secure OTAZ transmission using a node (i.e., | | | |
| FDD 163 | The OTAZ command shall zeroize or disable keys in the target equipment. | | | |
| FDD 164 | The OTAZ message shall provide Type 1 high grade authentication of the source and content of the transmission. | | | |
| FDD 165 | The JTRS WNW shall use RF spectrum that satisfies technical, operational and regulatory requirements for worldwide operation. | | | |

| Requirement # | Requirement Description | Build 1 | Build 2 | Build 3 |
|---|---|---|---|---|
| FDD 166 | With respect to these spectrum regulations, the WNW operating frequency range shall include frequency bands allocated to the mobile radio communications service that are authorized for military use. | | | |
| FDD 167 | Since the frequency bands satisfying these criteria may vary by region, the WNW and JTR sets shall incorporate adequate flexibility with respect to operating frequency, bandwidth, modulation, and power to address a range of possible host nation restrictions. | | | |

# Appendix F

## WNW Network Manager Information Exchange Requirements

| **Message Category** | **Sender** | **Receiver** | **Message** | **High-Level Description** |
|---|---|---|---|---|
| Network Planning | External Network Manager | WNW NM | IP Address Allotment | Allotment of IP addresses for use within the WNW network. |
| Network Planning | WNW NM | External Network Manager | Network Element Locations | Initial planning location of WNW network elements and interconnections among those elements. |
| Network Planning | External Network Manager | WNW NM | Router Configurations | Configuration information to enable routing between the WNW and external networks. |
| Spectrum Mgmt | External Network Manager | WNW NM | Frequency allotment | Allotment of frequencies for assignment by the WNW. |
| Spectrum Mgmt | WNW NM | External Network Manager | *Frequency usage* | Describes the frequencies actually being used within the network. |
| Spectrum Mgmt | WNW NM | External Network Manager | Equipment Settings | Specific RF settings for deployed radios (e.g., power, bandwidth). |
| IA | External Network Manager | WNW NM | IA Policies and Settings | IA policies and settings for the current operations. |
| IA | External Network Manager | WNW NM | IA Attack Alert | Indication/alert of possible IA attack (change in IA settings) |
| IA | WNW NM | External Network Manager | IA Attack Alert | Indication of possible IA attack |
| Network Monitoring | WNW NM | External Network Manager | Network status | Current status of WNW equipment and transmission links. |
| Network Monitoring | External Network Manager | WNW NM | Network status | Current status of external equipment and transmission links of interest to the WNW. |
| Network Monitoring | WNW NM | External Network Manager | Network Position | Current position of the WNW network elements plus connectivity. |
| Network | WNW NM | External Network | Performance Data | Data related to the performance of the WNW |

| **Message Category** | **Sender** | **Receiver** | **Message** | **High-Level Description** |
|---|---|---|---|---|
| Monitoring | | Manager | | equipment and transmission links. This could include throughput, link performance, BER, dropped packets, etc. |
| Fault Mgmt | WNW NM | External Network Manager | Trouble Ticket | Trouble tickets associated with WNW network faults. |
| Fault Mgmt | External Network Manager | WNW NM | Trouble Ticket | Trouble tickets associated with external network faults. |
| Account Mgmt | External Network Manager | WNW NM | User Profile Request | Data associated with requested accounts on the external network such as permissions, utilization limits, etc. |
| Account Mgmt | WNW NM | External Network Manager | Account Data | WNW users information. |